

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-085059

(43)Date of publication of application : 20.03.2003

(51)Int.Cl.

G06F 13/00

G06F 15/00

H04L 12/46

H04L 12/66

(21)Application number : 2002-068762

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 13.03.2002

(72)Inventor : KOKADO TAKESHI  
OKADA YASUNORI  
KUBOTA KOJI  
SAITO TAKAHIRO  
ISHIKAWA HIROKAZU

(30)Priority

Priority number : 2001076507  
2001199977

Priority date : 16.03.2001  
29.06.2001

Priority country : JP

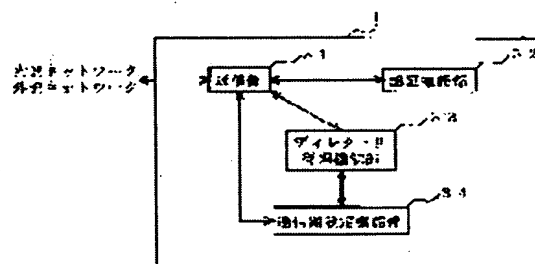
JP

## (54) FIREWALL SETTING METHOD AND SYSTEM FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a firewall setting method and a system therefor that limit users having access from an external network for each terminal of an internal network and allow the users to connect to a terminal of the internal network selectively.

SOLUTION: An HGW 1 has a communication part 31, an authentication function part 32, a directory management function part 33 and a channel setting function part 34. The communication part 31 receives data communication to the HGW 1. The authentication function part 32 determines whether the data are from an authentic user or not. The directory management function part 33 receives a service registration, registers it in service information, checks accordance with service publicity policy and requests the channel setting function part 34 to set a channel. The channel setting function part 34 monitors a data communication state on the channel to cancel the setting of an unnecessary channel.



## LEGAL STATUS

[Date of request for examination]

27.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-85059

(P 2 0 0 3 - 8 5 0 5 9 A)

(43) 公開日 平成15年 3月20日 (2003. 3. 20)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)	
G06F 13/00	351	G06F 13/00	351	Z 5B085
15/00	330	15/00	330	A 5B089
H04L 12/46		H04L 12/46		E 5K030
12/66		12/66		B 5K033

審査請求 未請求 請求項の数32 O L (全49頁)

(21) 出願番号	特願2002-68762 (P 2002-68762)	(71) 出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22) 出願日	平成14年 3月13日 (2002. 3. 13)	(72) 発明者	古門 健 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(31) 優先権主張番号	特願2001-76507 (P2001-76507)	(72) 発明者	岡田 恭典 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(32) 優先日	平成13年 3月16日 (2001. 3. 16)	(74) 代理人	100098291 弁理士 小笠原 史朗
(33) 優先権主張国	日本 (J P)		
(31) 優先権主張番号	特願2001-199977 (P2001-199977)		
(32) 優先日	平成13年 6月29日 (2001. 6. 29)		
(33) 優先権主張国	日本 (J P)		

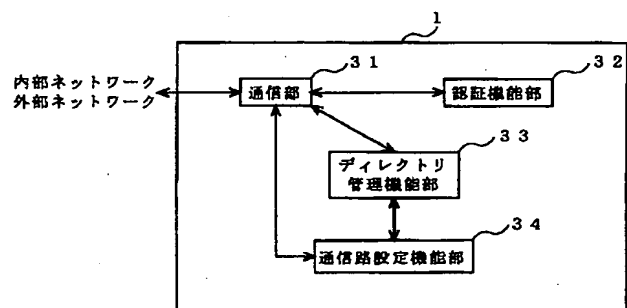
最終頁に続く

(54) 【発明の名称】 ファイアウォール設定方法およびその装置

(57) 【要約】

【課題】 内部ネットワークの端末毎に外部ネットワークからアクセス可能な使用者を限定し、また、上記使用者が選択的に内部ネットワークの端末に接続可能なファイアウォール設定方法およびその装置を提供する。

【解決手段】 HGW1は、通信部31、認証機能部32、ディレクトリ管理機能部33および通信路設定機能部34が設けられている。通信部31は、HGW1へのデータ通信を受信する。また、認証機能部32は、正当なユーザからのデータか否かを認証する。そして、ディレクトリ管理機能部33は、サービス登録を受け、サービス情報に登録し、サービス公開ポリシーとの対応をチェックし、通信路設定機能部34に通信路の設定を依頼する。また、通信路設定機能部34は、上記通信路のデータ通信状況を監視し、不要な通信路の設定を解除する。



## 【特許請求の範囲】

【請求項 1】 外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、

前記外部端末から送信され少なくとも外部端末が有する外部アドレスと前記外部端末の利用者を識別するユーザ識別データとを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理部と、

前記データ処理部で設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続するスイッチ部とを備え、

前記データ処理部は、

少なくとも前記通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、

前記ユーザ識別データを認証する認証機能部と、

前記サーバが有する内部アドレスとサービス種別と前記サーバに接続可能な外部の利用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、前記認証機能部で認証を受けた利用者に対して接続可能な前記サービス情報から選択させるディレクトリ管理機能部と、

前記ディレクトリ管理機能部で前記サービス情報から選択された前記サーバの前記内部アドレスと前記外部端末の前記外部アドレスとを用いて前記通信路を設定する通信路設定機能部とを含む、ファイアウォール装置。

【請求項 2】 前記ディレクトリ管理機能部に登録されている前記サービス情報は、前記サーバから送信され少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータによって登録されることを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 3】 前記サービスデータは、前記サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、

前記ディレクトリ管理機能部の前記サービス情報は、前記サービス抹消データによって該当するサービスが抹消されることを特徴とする、請求項 2 に記載のファイアウォール装置。

【請求項 4】 前記サービスデータは、前記公開先データを変更する公開先変更データをさらに含み、前記ディレクトリ管理機能部の前記サービス情報は、前記公開先変更データによって該当するサービスに接続可能な外部の利用者が変更されることを特徴とする、請求項 2 に記載のファイアウォール装置。

【請求項 5】 前記サービスデータは、前記サーバを固定的に識別するサーバ識別情報をさらに含み、前記ディレクトリ管理機能部は、前記サービス情報を前記サーバ識別情報に基づいて関連付けられた前記内部アドレスを更新することを特徴とする、請求項 2 に記載のフ

ファイアウォール装置。

【請求項 6】 前記ディレクトリ管理機能部に登録されている前記サービス情報は、前記ディレクトリ管理機能部が前記サーバから取得する、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 7】 前記ディレクトリ管理機能部は、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて前記サービス情報を登録し、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、前記サービスデータに係る公開先データを自動生成することを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 8】 前記ディレクトリ管理機能部は、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項 7 に記載のファイアウォール装置。

【請求項 9】 前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに生成することを特徴とする、請求項 7 に記載のファイアウォール装置。

【請求項 10】 前記ディレクトリ管理機能部は、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データの数が所定数以上である場合

には、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに作成し、一方、当該選出された公開先データの数が所定数以上でない場合には、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項 7 に記載のファイアウォール装置。

【請求項 11】 前記ディレクトリ管理機能部への前記サービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 12】 前記通信路設定機能部は、さらに設定した前記通信路を通るデータを監視し、予め設定された期間に前記通信路をデータが通らないとき、前記通信路を解除することを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 13】 前記通信路設定機能部は、前記外部端末から送信され前記サーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 14】 前記通信路設定機能部は、前記サーバから送信され前記外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項 1 に記載のファイアウォール装置。

【請求項 15】 外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、  
前記サーバから送信され少なくとも前記サーバが有する内部アドレスとサービス種別とが含まれたサービスデータを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理部と、  
前記データ処理部で設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続するスイッチ部とを備え、  
前記データ処理部は、  
少なくとも前記サービスデータを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、  
前記内部アドレスと前記サービス種別と前記サーバに接続可能な前記外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理機能部と、  
前記サービス情報が登録された時に、前記公開先データに該当する前記外部端末が有する外部アドレスと前記サーバの前記内部アドレスとを用いて前記通信路を設定する通信路設定機能部を含む、ファイアウォール装置。  
【請求項 16】 前記ディレクトリ管理機能部に設定さ

れる前記公開先データは、前記サーバに対して全ての前記外部端末が接続可能であることを特徴とする、請求項 15 に記載のファイアウォール装置。

【請求項 17】 外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、

前記外部端末から送信され少なくとも外部端末が有する外部アドレスと前記外部端末の利用者を識別するユーザ識別データとを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、

前記データ処理ステップで設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続する接続ステップとを備え、

前記データ処理ステップは、

少なくとも前記通信データを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、

前記ユーザ識別データを認証する認証ステップと、

前記サーバが有する内部アドレスとサービス種別と前記サーバに接続可能な外部の利用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、前記認証ステップで認証を受けた利用者に対して接続可能な前記サービス情報から選択させるディレクトリ管理ステップと、

前記ディレクトリ管理ステップで前記サービス情報から選択された前記サーバの前記内部アドレスと前記外部端末の前記外部アドレスとを用いて前記通信路を設定する通信路設定ステップを含む、ファイアウォール設定方法。

【請求項 18】 前記ディレクトリ管理ステップに登録されている前記サービス情報は、前記サーバから送信され少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータによって登録されることを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 19】 前記サービスデータは、前記サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、

前記ディレクトリ管理ステップの前記サービス情報は、前記サービス抹消データによって該当するサービスが抹消されることを特徴とする、請求項 18 に記載のファイアウォール設定方法。

【請求項 20】 前記サービスデータは、前記公開先データを変更する公開先変更データをさらに含み、  
前記ディレクトリ管理ステップの前記サービス情報は、前記公開先変更データによって該当するサービスに接続可能な外部の利用者が変更されることを特徴とする、請求項 18 に記載のファイアウォール設定方法。

【請求項 21】 前記サービスデータは、前記サーバを

固定的に識別するサーバ識別情報をさらに含み、前記ディレクトリ管理ステップは、前記サービス情報を前記サーバ識別情報に基づいて関連付けられた前記内部アドレスを更新することを特徴とする、請求項 18 に記載のファイアウォール設定方法。

【請求項 22】 前記ディレクトリ管理ステップにおいて登録される前記サービス情報は、前記ディレクトリ管理ステップにおいて前記サーバから取得する、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 23】 前記ディレクトリ管理ステップは、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて前記サービス情報を登録し、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、前記サービスデータに係る公開先データを自動生成することを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 24】 前記ディレクトリ管理ステップは、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項 23 に記載のファイアウォール設定方法。

【請求項 25】 前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに生成することを特徴とする、請求項 23 に記載のファイアウォール設定方法。

【請求項 26】 前記ディレクトリ管理ステップは、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、

前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレ

トリ管理ステップにおいて未登録である場合、前記ディレクトリ管理ステップは、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データの数 が所定数以上である場合には、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに作成し、一方、当該選出された公開先データの数 が所定数以上でない場合には、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項 23 に記載のファイアウォール設定方法。

【請求項 27】 前記ディレクトリ管理ステップへの前記サービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 28】 前記通信路設定ステップは、さらに設定した前記通信路を通るデータを監視し、予め設定された期間に前記通信路をデータが通らないとき、前記通信路を解除することを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 29】 前記通信路設定ステップは、前記外部端末から送信され前記サーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 30】 前記通信路設定ステップは、前記サーバから送信され前記外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項 17 に記載のファイアウォール設定方法。

【請求項 31】 外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、

前記サーバから送信され少なくとも前記サーバが有する内部アドレスとサービス種別とが含まれたサービスデータを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、

前記データ処理ステップで設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続する接続ステップとを備え、

前記データ処理ステップは、

少なくとも前記サービスデータを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、

前記内部アドレスと前記サービス種別と前記サーバに接続可能な前記外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレ

10

20

30

40

50

トリ管理ステップと、

前記サービス情報が登録された時に、前記公開先データに該当する前記外部端末が有する外部アドレスと前記サーバの前記内部アドレスとを用いて前記通信路を設定する通信路設定ステップとを含む、ファイアウォール設定方法。

【請求項 32】 前記ディレクトリ管理ステップに設定される前記公開先データは、前記サーバに対して全ての前記外部端末が接続可能であることを特徴とする、請求項 31 に記載のファイアウォール設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、外部ネットワークから内部ネットワークへの不正アクセスの遮断に関し、より特定的には、ファイアウォール設定方法およびその装置に関する。

【0002】

【従来の技術】従来、インターネット等の外部ネットワークと LAN (Local Area Network) 等の内部ネットワークとの間にファイアウォール装置を設置することで、データ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを防御している。このファイアウォール装置の一つにパケットフィルタリングルーター型がある。このパケットフィルタリングルーター型は、内部ネットワークと外部ネットワークとの間で通信されるパケットをある規則に従って転送したりブロックしたりする。しかしながら、このファイアウォール装置も万全ではなく、ネットワークやコンピュータシステムに対する物理的または論理的な侵入や破壊から防止するためのセキュリティ対策の重要性が増している。

【0003】一方、ローカルアドレス (Local Address: 以下、LA とする) と呼ばれる内部ネットワークの IP アドレス (Internet Protocol Address) は、外部ネットワークに対しては有効ではないため、アドレス変換によって外部ネットワークに対して有効なグローバルアドレス (Global Address: 以下、GA とする) に変換される。このアドレス変換に改良を加えた技術として IP マスカレード (Masquerade) がある。この IP マスカレードでは、上位プロトコルである TCP/UDP の通信ポート番号を識別し、LA と GA との対応関係を管理することで、1 つの GA で複数の LA が同時に通信可能になる。

【0004】上記のように内部ネットワークに複数の端末を持ち、GA が共有可能なネットワークアドレス変換方法が、特開 2000-59430 号公報に開示されている。この方法は、内部ネットワークの端末と外部ネットワークに接続された端末とがポート番号を変換せずに通信可能とすることを目的としている。この方法による

と、アドレス変換装置にアドレス変換のルールを示す内部テーブルを持たせ、その内部テーブルに、内部ネットワークの端末が通信に用いるポート番号 (LP) および外部ネットワークの端末の IP アドレス (IA) の対 (LP、IA) と、内部ネットワークの端末の IP アドレス (LA) との対応関係を記憶する。したがってこのアドレス変換装置では、上記内部テーブルの設定によって、内部ネットワークの端末毎に、アクセス可能な外部ネットワークの端末を限定することができる。このようなアドレス変換方法をファイアウォール装置に導入することにより、内部ネットワークの端末毎にアクセス可能な外部ネットワークの端末を限定するというセキュリティ対策が実現できる。

【0005】一方、さまざまな機器がネットワークで接続される状況において、ユーザがネットワークに接続されている機器を操作して、他のネットワークに接続されている機器の制御情報や状態情報などのサービス情報を入手してその機器を制御することが考えられる。しかし、ネットワークに属しているすべてのユーザに対し、ネットワーク上に提供されているすべてのサービス情報を提供して機器の制御を可能とすることは、ネットワークの安全上好ましくないと考えられる。

【0006】この問題に対して、従来、ネットワークに属するユーザ毎に異なるサービスの情報を提供するネットワークサービス管理方式が、特開平 11-275074 号公報において開示されている。このネットワークサービス管理方式によれば、ネットワークに発生した情報を、ユーザに対して提供する場合、ユーザの業務内容によって、異なる内容を提供する方法を示している。この方式の例では、ユーザはネットワーク管理者、サービス管理者、ユーザに分類され、図 51 に示されるネットワークが存在する場合、ネットワーク管理者に対しては、図 52 に示されるネットワーク全体の情報を提供し、サービス管理者に対しては、図 53 に示されるサービスの情報を提供し、ユーザに対しては、図 54 に示されるサーバからユーザへのパスのみを提供する。

【0007】

【発明が解決しようとする課題】しかしながら、上記アドレス変換方法は、内部ネットワークの端末にアクセス可能な外部ネットワークの端末装置を限定するのみである。つまり、アクセスが許可されている外部ネットワークの端末装置からは正規の利用者に限らず誰でも (悪意のある第三者も) 内部ネットワークの端末にアクセス可能である。よって上記アドレス変換方法はセキュリティで劣る面がある。また、複数の使用者が同じ外部ネットワーク端末装置を用いる場合、使用者が変わってもアクセスできる内部ネットワーク端末は同じであり、使用者毎に異なる内部ネットワーク端末に接続することができない。さらに、内部ネットワークに同じサービスを提供するサーバ (例えば、FTP サーバ) が複数ある場合、

使用者が接続することのできるサーバが1つに固定されてしまい、使用者はこれらのサーバに選択的に接続することができない。また、例えば外部ネットワークの端末装置が電話回線網に接続されている場合などでは外部ネットワークの端末装置を区別するために用いられている I A が固定値でないので、上記 I A が変更される毎に上記内部テーブルを再設定する必要がある。しかしこの再設定作業は非常に困難であり、固定値でない I A に対するアドレス変換は容易ではなかった。

【0008】それ故に、本発明の目的は、内部ネットワークの端末毎に外部ネットワークからアクセス可能な使用者を限定し、また、上記使用者が選択的に内部ネットワークの端末に接続することを可能にするためのファイアウォール設定方法およびその装置を提供することである。

【0009】また、上記機器制御方式においては、ネットワークにユーザもしくはサービスなど、新たな構成要素が追加された場合、この構成要素に対して、提供してよい項目を設定しなくてはならない。このことは、家庭内のネットワークについても当てはまり、例えば、ネットワークに対して十分な知識を持たないユーザが、ネットワークに機器を接続する際にその設定を行う必要に迫られる。また、ネットワークに対して提供してよい項目を不用意に選択すると、宅外から無制限にアクセスが可能になるなど、ネットワークの安全上、好ましくない事態が起こりうる。

【0010】それ故に、本発明の他の目的は、ネットワークに新たな構成要素を加える場合に、単に機器を接続するだけで、好ましいアクセス制限の設定がなされ、セキュリティを確保できる装置および方法を提供することである。

【0011】

【課題を解決するための手段および発明の効果】上記目的を達成するために、本発明は、以下に述べるような特徴を有している。第1の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、外部端末から送信され少なくとも外部端末が有する外部アドレスと外部端末の利用者を識別するユーザ識別データとを含んだ通信データを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理部と、データ処理部で設定された通信路に基づいて、サーバと外部端末とを接続するスイッチ部とを備え、データ処理部は、少なくとも通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、ユーザ識別データを認証する認証機能部と、サーバが有する内部アドレスとサービス種別とサーバに接続可能な外部の利用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、認証機能部で認証を受けた使用者に対

して接続可能なサービス情報から選択させるディレクトリ管理機能部と、ディレクトリ管理機能部でサービス情報から選択されたサーバの内部アドレスと外部端末の外部アドレスとを用いて通信路を設定する通信路設定機能部とを含む。

【0012】第1の発明によれば、外部から接続可能な外部ユーザを限定しユーザ認証を確認した後、その外部ユーザが使用している外部端末の外部アドレスを取得し、その外部アドレスを基にして通信路を設定している。したがって、内部ネットワークのサービスに対して、外部からアクセス可能な外部ユーザを限定して公開することができる。また、上記外部ユーザが使用する外部端末を変更する、あるいは外部ユーザが使用している外部端末の外部アドレスが変わっても同様のアクセスが可能である。また、上記外部ユーザは、通信路を設定する要求をするとき、アクセス可能なサービスを選択的に接続することができ、さらに、同じサービスを内部ネットワーク内で複数のサーバが有していても、上記外部ユーザは上記サーバを選択的に接続することができる。一方、内部ネットワークのサーバに接続可能な外部ユーザを、そのサーバのサービス毎に設定できるため、内部ネットワークの中で同一のサービスを有する複数のサーバに対して、それぞれの異なった接続可能な外部ユーザを設定することにより、サーバ毎のセキュリティレベルを容易に設定することができる。

【0013】第2の発明は、第1の発明に従属する発明であって、ディレクトリ管理機能部に登録されているサービス情報は、サーバから送信され少なくとも内部アドレスとサービス種別とが含まれたサービスデータによって登録されることを特徴とする。

【0014】第2の発明によれば、内部ネットワークに接続されているサーバからの指示により、外部ネットワークに公開するサービスを登録および変更することができる。

【0015】第3の発明は、第2の発明に従属する発明であって、サービスデータは、サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、ディレクトリ管理機能部のサービス情報は、サービス抹消データによって該当するサービスが抹消されることを特徴とする。

【0016】第3の発明によれば、内部ネットワークのサーバから、そのサーバのサービス毎に外部に提供するか否かを指示することができる。

【0017】第4の発明は、第2の発明に従属する発明であって、サービスデータは、公開先データを変更する公開先変更データをさらに含み、ディレクトリ管理機能部のサービス情報は、公開先変更データによって該当するサービスに接続可能な外部の利用者が変更されることを特徴とする。

【0018】第4の発明によれば、内部ネットワークか



ら、そのサーバのサービスに接続可能な外部ユーザを変更し設定することができる。

【0019】第5の発明は、第2の発明に従属する発明であって、サービスデータは、サーバを固定的に識別するサーバ識別情報をさらに含み、ディレクトリ管理機能部は、サービス情報をサーバ識別情報に基づいて関連付けられた内部アドレスを更新することを特徴とする。

【0020】第5の発明によれば、内部ネットワークのサーバの内部アドレスが変更された場合、上記サーバを識別する固定値を認識することにより、上記サーバと変更された上記内部アドレスとを対応させることができるため、内部アドレス変換時に必要なテーブルの変更を自動的に容易に処理することができる。

【0021】第6の発明は、第1の発明に従属する発明であって、ディレクトリ管理機能部に登録されているサービス情報は、ディレクトリ管理機能部がサーバから取得する、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする。

【0022】第6の発明によれば、内部ネットワークに接続されているサーバからの指示によらず、外部ネットワークに公開するサービスを登録および変更することができる。

【0023】第7の発明は、第1の発明に従属する発明であって、ディレクトリ管理機能部は、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいてサービス情報を登録し、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、サービスデータに係る公開先データを自動生成することを特徴とする。

【0024】第7の発明によれば、ネットワーク上に新たなサーバが接続されたときなどに、その公開先データが登録されていない場合であっても、これを動的に作成するため、ユーザがその都度設定を行う必要がない。

【0025】第8の発明は、第7の発明に従属する発明であって、ディレクトリ管理機能部は、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【0026】第8の発明によれば、公開先データが存在しない場合に、予め設定された初期公開先データに基づいて好ましい公開先データを生成することができる。

【0027】第9の発明は、第7の発明に従属する発明であって、サーバが有する内部アドレスとサービス種別

とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【0028】第9の発明によれば、公開先データが存在しない場合に、すでに登録されている公開先データに基づいて好ましい公開先データを生成することができる。

【0029】第10の発明は、第7の発明に従属する発明であって、ディレクトリ管理機能部は、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理機能部に存在しない場合、ディレクトリ管理機能部は、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データの数が所定数以上である場合には、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに作成し、一方、この選出された公開先データの数が所定数以上でない場合には、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【0030】第10の発明によれば、公開先データが存在しない場合に、この公開先データを類推するための他の公開先データが、一定数以上存在する場合にはそれらから類推して公開先データを生成し、一方、一定数以上存在しない場合には、初期公開先データに基づいて生成する。よって、公開先データを類推するための材料となる他の公開先データが少ない場合に不十分な判断材料に基づいて望ましくない設定がなされてしまう危険が回避できる。

【0031】第11の発明は、第1の発明に従属する発明であって、ディレクトリ管理機能部へのサービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする。

【0032】第11の発明によれば、外部ネットワークに提供可能なサービスに対して有効期限を設けており、上記サービスが有効である時のみ一時的に通信路を設定し、しかも上記サービス専用の通信路であるため、さらにセキュリティの向上を実現できる。

【0033】第12の発明は、第1の発明に従属する発明であって、通信路設定機能部は、さらに設定した通信路を通るデータを監視し、予め設定された期間に通信路をデータが通らないとき、通信路を解除することを特徴とする。

10

20

30

40

50

【0034】第12の発明によれば、外部ネットワークに提供可能なサービスの通信路が設けられた後、上記サービスに対して予め設定した期間に上記通信路が外部ユーザによって使用されない場合、上記通信路を解除するため、さらにセキュリティの向上を実現できる。

【0035】第13の発明は、第1の発明に従属する発明であって、通信路設定機能部は、外部端末から送信されサーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【0036】第14の発明は、第1の発明に従属する発明であって、通信路設定機能部は、サーバから送信され外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【0037】第13および第14の発明によれば、外部端末あるいはサーバからサービス通信終了データを受信することにより通信路を解除するため、サービスの公開が不要な期間の外部からのアクセスを防止することができる。

【0038】第15の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、サーバから送信され少なくともサーバが有する内部アドレスとサービス種別とが含まれたサービスデータを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理部と、データ処理部で設定された通信路に基づいて、サーバと外部端末とを接続するスイッチ部とを備え、データ処理部は、少なくともサービスデータと通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、内部アドレスとサービス種別とサーバに接続可能な外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理機能部と、サービス情報が登録された時に、公開先データに該当する外部端末の外部アドレスとサーバの内部アドレスとを用いて通信路を設定する通信路設定機能部とを含む。

【0039】第15の発明によれば、サーバの指示によってディレクトリ管理機能部にサービス情報を登録されたときに、外部端末からの通信データがなくても、設定された公開先に対して通信路を設定することができる。

【0040】第16の発明は、第15の発明に従属する発明であって、ディレクトリ管理機能部に設定される公開先データは、サーバに対して全ての外部端末が接続可能であることを特徴とする。

【0041】第16の発明によれば、内部ネットワークのサーバが有するサービスを、外部端末を限定せずに公開することができる。

【0042】第17の発明は、外部ネットワークを介し

て外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、外部端末から送信され少なくとも外部端末が有する外部アドレスと外部端末の利用者を識別するユーザ識別データとを含んだ通信データを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、データ処理ステップで設定された通信路に基づいて、サーバと外部端末とを接続する接続ステップとを備え、データ処理ステップは、少なくとも通信データを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、ユーザ識別データを認証する認証ステップと、サーバが有する内部アドレスとサービス種別とサーバに接続可能な外部の利用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、認証ステップで認証を受けた利用者に対して接続可能なサービス情報から選択させるディレクトリ管理ステップと、ディレクトリ管理ステップでサービス情報から選択されたサーバの内部アドレスと外部端末の外部アドレスとを用いて通信路を設定する通信路設定ステップとを含む。

【0043】第18の発明は、第17の発明に従属する発明であって、ディレクトリ管理ステップに登録されているサービス情報は、サーバから送信され少なくとも内部アドレスとサービス種別とが含まれたサービスデータによって登録されることを特徴とする。

【0044】第19の発明は、第18の発明に従属する発明であって、サービスデータは、サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、ディレクトリ管理ステップのサービス情報は、サービス抹消データによって該当するサービスが抹消されることを特徴とする。

【0045】第20の発明は、第18の発明に従属する発明であって、サービスデータは、公開先データを変更する公開先変更データをさらに含み、ディレクトリ管理ステップのサービス情報は、公開先変更データによって該当するサービスに接続可能な外部の利用者が変更されることを特徴とする。

【0046】第21の発明は、第18の発明に従属する発明であって、サービスデータは、サーバを固定的に識別するサーバ識別情報をさらに含み、ディレクトリ管理ステップは、サービス情報をサーバ識別情報に基づいて関連付けられた内部アドレスを更新することを特徴とする。

【0047】第22の発明は、第17の発明に従属する発明であって、ディレクトリ管理ステップにおいて登録されるサービス情報は、ディレクトリ管理ステップにおいてサーバから取得する、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする。

10

20

30

40

50

【0048】第23の発明は、第17の発明に従属する発明であって、ディレクトリ管理ステップは、少なくとも内部アドレスとサービス種別とが含まれたサービスデータに基づいてサービス情報を登録し、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理機ステップは、サービスデータに係る公開先データを自動生成することを特徴とする。

【0049】第24の発明は、第23の発明に従属する発明であって、ディレクトリ管理ステップは、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理ステップは、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【0050】第25の発明は、第23の発明に従属する発明であって、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理ステップは、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【0051】第26の発明は、第23の発明に従属する発明であって、ディレクトリ管理ステップは、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納ステップを含み、サーバが有する内部アドレスとサービス種別とに関連付けられる公開先データがディレクトリ管理ステップにおいて未登録である場合、ディレクトリ管理ステップは、現時点において管理している公開先データの中から、サービスデータに対して一部の条件を除いて条件が一致する公開先データを選出し、この選出された公開先データの数が所定数以上である場合には、この選出された公開先データに基づいて、このサービスデータに係る公開先データを新たに作成し、一方、この選出された公開先データの数が所定数以上でない場合には、初期公開先データに基づいて、このサービスデータに係る公開先データを新たに生成することを特徴とする。

【0052】第27の発明は、第17の発明に従属する発明であって、ディレクトリ管理ステップへのサービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする。

【0053】第28の発明は、第17の発明に従属する発明であって、通信路設定ステップは、さらに設定した通信路を通るデータを監視し、予め設定された期間に通信路をデータが通らないとき、通信路を解除することを特徴とする。

【0054】第29の発明は、第17の発明に従属する発明であって、通信路設定ステップは、外部端末から送信されサーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【0055】第30の発明は、第17の発明に従属する発明であって、通信路設定ステップは、サーバから送信され外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、通信路を解除することを特徴とする。

【0056】第31の発明は、外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、サーバから送信され少なくともサーバが有する内部アドレスとサービス種別とが含まれたサービスデータを処理し、サーバおよび外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、データ処理ステップで設定された通信路に基づいて、サーバと外部端末とを接続する接続ステップとを備え、データ処理ステップは、少なくともサービスデータを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、内部アドレスとサービス種別とサーバに接続可能な外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理ステップと、サービス情報が登録された時に、公開先データに該当する外部端末が有する外部アドレスとサーバの内部アドレスとを用いて通信路を設定する通信路設定ステップとを含む。

【0057】第32の発明は、第31の発明に従属する発明であって、ディレクトリ管理ステップに設定される公開先データは、サーバに対して全ての外部端末が接続可能であることを特徴とする。

【0058】

【発明の実施の形態】（第1の実施形態）図1は、本発明の第1の実施形態に係るファイアウォール装置の基本的構成を示す図である。以下、図1を用いて、当該実施形態について説明する。

【0059】図1において、当該実施形態では、内部ネットワークとして、ホームゲートウェイ装置（以下、HGWとする）1に複数のサーバ2-1～nがバス接続されてLANが構築されている。一方、HGW1は、外部ネットワークとして、インターネット網を介して複数の外部端末3を接続されている。なお、内部ネットワークには、サーバ2-1～nの他に、内部端末が接続されていてもかまわないし、外部ネットワークには、外部端末

3の他に、外部サーバが接続されていてもかまわない。

【0060】ここで、HGW1は、外部ネットワークとの送受信に用いられるグローバルIPアドレス（GA）が付与されており、複数のポート番号（GP）を用いてパケットの送受信を行う。また、サーバ2-1～nは、それぞれに固有のローカルIPアドレス（LA）1～nとサーバ2-1～nが提供するサービスに応じて、クライアントとなる端末からの通信を受信するポート番号（LP）1～nが設定されている。さらに、外部端末3は、外部ネットワークとの送受信に用いられるグローバルIPアドレス（IA）と送受信に使用するポート番号（IP）とが付与されている。

【0061】次に、前述したHGW1の内部ハードウェアの基本構成について説明する。なお、図2は、当該実施形態に係るHGW1の内部ハードウェア基本構成を示すブロック図である。以下、図2を参照して、HGW1について説明する。

【0062】図2において、HGW1は、CPU10とメモリ11とIPスイッチ部20とを備えている。また、IPスイッチ部20は、コントローラ21、メモリ22、IPフィルタ機能部23、フォワーディング機能部24、アドレス変換機能部25およびPHY・MAC（Physical Layer Protocol・Media Access Control）機能部26aおよび26bを含んでいる。CPU10は、各機能部の制御や送受信するデータの処理等を行い、メモリ11には、HGW1の動作プログラムやデータ等が格納されている。また、コントローラ21は、CPU10から設定情報を受け取り、上記設定情報に基づいてIPフィルタ機能部23、フォワーディング機能部24およびアドレス変換機能部25の設定を行う。また、コントローラ21は、外部ネットワークおよび内部ネットワークに対してデータの送受信を行うPHY・MAC機能部26で受信したデータに対して、IPフィルタ機能部23、フォワーディング機能部24およびアドレス変換機能部25に処理を指示する。メモリ22は、PHY・MAC機能部26で受信したパケットデータを一時的に格納する。IPフィルタ機能部23は、その内部にフィルタ条件格納用のレジスタを有し、上記レジスタに格納されたフィルタ条件に基づいて、メモリ22に格納された上記パケットデータのチェックを行う。なお、上記パケットデータが、上記フィルタ条件に対して許可されないデータである場合、IPフィルタ機能部23は、上記パケットデータを廃棄する。フォワーディング機能部24は、その内部にフォワーディング情報格納用のレジスタを有し、上記レジスタに格納された上記情報に基づいて、メモリ22に格納されたパケットデータの転送先PHY・MAC機能部26を決定し、上記パケットデータの転送を制御する。アドレス変換機能部25は、その内部にアドレス変換情報格納用のレジスタを有し、上記レ

ジスタに格納された上記アドレス変換情報に基づいて、メモリ22に格納されたパケットデータに対してIPアドレスの変換を行う。

【0063】次に、前述したHGW1のソフトウェアの基本構成について説明する。なお、図3は、当該実施形態に係るHGW1のソフトウェア基本構成を示すブロック図である。以下、図3を参照して、HGW1について説明する。

【0064】図3において、HGW1は、通信部31、認証機能部32、ディレクトリ管理機能部33および通信路設定機能部34が設けられている。通信部31は、外部端末3またはサーバ2からHGW1へのデータ通信を受信し、データ内容によって各機能部に処理を依頼する。また、認証機能部32は、認証情報を管理し、上記データが正当なユーザからのデータか否かを認証する。そして、ディレクトリ管理機能部33は、サーバ2からのサービス登録を受け、サービス情報（詳細は、後述する）を登録および管理し、上記サービス情報とサービス公開ポリシー（詳細は、後述する）との対応をチェックし、必要に応じて通信路設定機能部34に通信路の設定を依頼する。また、通信路設定機能部34は、IPフィルタ機能部23、フォワーディング機能部24、アドレス変換機能部25およびアプリケーションGW等を設定し、通信路を設定する。また、通信路設定機能部34は、上記通信路のデータ通信状況を監視し、不要な通信路の設定を解除する。

【0065】ここで、当該ファイアウォール装置は、HGW1のスイッチ部20に通信路を設定することにより外部ネットワークの外部端末3と内部ネットワークのサーバ2とが接続可能となり、サーバ2のサービスが外部に公開される。上記内部ネットワークのサーバ2から公開可能なサービスについては、サービス情報（詳細は、後述する）として管理されており、上記サービス情報に基づいて、通信路が設定される。当該ファイアウォール装置では、上記公開の方法として、外部ユーザの認証を必要としない「認証なし」のサービスと、外部ユーザの認証を必要とする「認証後公開」のサービスと、外部ネットワークに公開されない「非公開」のサービスとを設定できる。上記「認証なし」のサービスは、上記サービス情報にそのサービスが登録された時点で通信路が設定され、外部ネットワークからどのようなユーザでも接続可能である。また、上記「認証後公開」のサービスは、許可されたユーザがそのサービスへ接続を希望した時点で通信路が一時的に設定され、許可されたユーザのみが接続可能である。さらに、上記公開可能なサービスは、それぞれ有効期限を有しており、その有効期限が終了した場合、上記サービス情報から抹消される。以下、上述したそれぞれの通信路設定処理について説明する。

【0066】まず、HGW1で行われる上記サービス情報の設定処理および上記「認証なし」のサービスに対す

る通信路設定処理について説明する。なお、図4および図5はHGW1で行われる通信路設定処理の動作を示すフローチャートであり、図8～図10はHGW1で行われる通信路設定処理の時に作成・使用される情報テーブルを示している。以下、図4、図5および図8～図10を参照して、通信路設定処理について説明する。

【0067】図4において、HGW1は、SMTP (Simple Mail Transfer Protocol)、FTP (File Transfer Protocol) およびHTTP (Hyper Text Transfer Protocol) 等のサービスをディレクトリ管理機能部33に登録するため、サーバ2からサービス登録を受信する(ステップS101)。

【0068】なお、ここではサーバ2がHGW1に対してサービス登録を行う場合について説明しているが、これに限らず、HGW1がサーバ2よりサービス情報を取得するようにしても構わない。その場合、ディレクトリ管理機能部33は、図4のステップS101の代わりに、図13に示す処理を実行する。つまり、ディレクトリ管理機能部33は、まず内部ネットワークに接続されているサーバ2に対してポートスキャンを行い、サーバ2が使用しているポートを検索する(S201)。この結果、サーバが使用しているポートが予めサービスの仕様によって決定されているポート(ウェルノウンポート: well-known port)であった場合には、そのポートに対応するサービスをサーバが提供していることが分かる(S202)。なおサーバが使用しているポートがウェルノウンポートでない場合には、ポートスキャンに対する応答メッセージを確認することにより、サーバが提供しているサービスを検知することができる。このとき、HGW1が新規サーバの接続を知る方法としては、DHCPによる新規IPアドレスの割当て時に検出する方法や、ARPパケットのMACアドレスを監視することによって検出する方法等がある。加えて、IPover1394を使用する場合のように、新規の機器接続を検出可能なネットワークを使用する場合には、HGW1は、ネットワークの仕組みを用いて新規サーバの接続を検出し、このサーバからサービス情報を取得する。

【0069】次に、HGW1は、受信した上記サービス登録のサービスに対して、ディレクトリ管理機能部33に格納されているサービス情報を参照して、上記サービスのサービス種別とサーバ識別情報との対が、既に上記サービス情報に登録済みか否かを判断する(ステップS102)。

【0070】図8は、ディレクトリ管理機能部33に格納されているサービス情報の一例を示す図である。サービス情報は、内部ネットワークのサーバ2がどのようなサービスを外部に公開可能であることを示す情報であり、スイッチ部20の通信路を設定するための情報も管理さ

れている。上記サービス情報は、サービス名、サービスアドレス、プロトコル、外部公開ポート番号(GP)、現在の公開先、サービス有効期間および状態を、互に関連付けたテーブルとしてディレクトリ管理機能部33に格納されている。サービス名は、外部に公開するサービス種別を示しており、サービスアドレスは、サーバ2のサーバ識別情報、LAおよびLPを示している。ここで、サーバ識別情報とは、MACアドレスやサーバ装置のシリアル番号等のサーバ2を識別する固定値である。また、現在の公開先は、HGW1のスイッチ部20で通信路が設定されている公開先を示している。なお、外部から接続可能なユーザまたは端末を限定して公開されている場合、現在の公開先は、そのユーザ名と外部端末3のIAおよびIPとが示される。サービス有効期間は、それぞれに予め設定されたサービス種別毎の公開有効期間の残存時間を示している。また、状態は、サービスが現在使用可であるか否かを示している。なお、このサービス情報へのサービス登録は、同じサービス種別であってもサーバ識別情報が異なる場合、登録済みとは判断されないため、新しいサービスとして処理される。したがって、上記サービス情報には、サーバ2毎に有効なサービスが登録されることになる。

【0071】ステップS102で、上記サービス登録のサービスに対してサービス種別とサーバ識別情報との対が、上記サービス情報に登録されていない場合、HGW1は、予めディレクトリ管理機能部33に設定されているサービス基本公開ポリシーに基づいて、サービス詳細公開ポリシーを設定する(ステップS109)。

【0072】図9はディレクトリ管理機能部33に予め設定されているサービス基本公開ポリシーの一例を示す図であり、図10はディレクトリ管理機能部33に設定されるサービス詳細公開ポリシーの一例を示す図である。まず、サービス基本公開ポリシーは、それぞれのサービス種別に対する外部から接続可能な条件として、公開先相手、公開条件および公開ポートが、予めディレクトリ管理機能部33に設定されている。なお、公開先相手は、外部から接続可能なユーザを限定して公開する場合、そのユーザ名が設定される。また、接続可能な外部端末3を限定して公開する場合、その端末のIAが設定される。そして、公開条件が「認証なし」で公開先相手が「全て公開」の場合、そのサービスは外部のどのようなユーザからも接続が可能となり、上記サービス情報にそのサービスが登録された時点でスイッチ部20の通信路が設定される。また、公開条件が「認証なし」で公開先相手が外部端末3のIAの場合、上記サービス情報にそのサービスが登録された時点でスイッチ部20の通信路が設定される。一方、公開条件が「認証後公開」の場合、公開先相手に登録されたユーザがそのサービスに接続を希望した時点でスイッチ部20の通信路が一時的に設定される。ステップS109では、上記基本公開ポリ

シーに基づいて、サーバ 2 毎に、それぞれサービス種別に対する上記接続条件をサービス詳細公開ポリシーとして設定する。したがって、上記サービス詳細公開ポリシーは、それぞれのサーバ 2 に対して上記接続条件が設定され、サーバ 2 の管理者によって環境に応じた上記接続条件に変更することが可能である。なお、上記接続条件の変更が不要な場合、サービス詳細公開ポリシーには、サービス基本公開ポリシーの上記接続条件が適用される。また、サービス基本公開ポリシーに該当するサービス種別がない場合、公開先相手は「非公開」として設定される。

【0073】次に、HGW1 は、上記サービス登録のサービスを上記サービス情報にエントリ追加し、上記サービスの内容を上記サービス情報に設定する（ステップ S110）。そして、HGW1 は、上記サービス詳細公開ポリシーを参照し、上記サービスの公開条件が「認証なし」か否かを判断する（ステップ S111）。HGW1 は、上記公開条件が「認証なし」でない場合、フローを終了し、上記公開条件が「認証なし」の場合、さらに上記サービス詳細公開ポリシーの公開ポートが「指定なし」か否かを判断する（ステップ S112）。そして、HGW1 は、上記公開ポートが「指定なし」の場合、空ポート番号（GP）を設定した後（ステップ S113）、ステップ S116 に進む。一方、上記公開ポートが指定されている場合、HGW1 は、指定されているポート（GP）が使用可か否かを判断する（ステップ S114）。そして、HGW1 は、指定されている GP が使用可の場合、その GP を取得した後（ステップ S115）、ステップ S116 に進む。次に、HGW1 は、上記サービス情報を参照して、上記サービスの状態が「使用可」か否かを判断し（ステップ S116）、上記状態が「使用不可」の場合、フローを終了する。上記状態が「使用可」で公開先相手が「全て公開」の場合、HGW1 は、上記サービスに対して内部アドレス情報（LA および LP）および外部公開用アドレス情報（HGW1 の GA および上記 GP）を取得して IP フィルタ機能部 23 およびアドレス変換機能部 25 を設定することによりスイッチ部 20 の通信路を設定し（ステップ S117）、フローを終了する。なお、ステップ S117 で、上記状態が「使用可」で公開先相手が外部端末 3 の IA の場合、HGW1 は、上記サービスに対して内部アドレス情報（LA および LP）、外部公開用アドレス情報（HGW1 の GA および上記 GP）および外部端末 3 のアドレス情報（外部端末 3 の IA および IP）を取得して IP フィルタ機能部 23 およびアドレス変換機能部 25 を設定することによりスイッチ部 20 の通信路を設定する。

【0074】一方、ステップ S114 で、指定されている GP が使用不可の場合、HGW1 は、上記サービス情報を参照して該当する上記サービスの状態を「使用不

可」に設定し（ステップ S118）、フローを終了する。これは、指定されたポート番号 GP を用いて、アドレス変換機能部 25 が設定できないことを意味する。例えば、同一の外部端末 3 が、FTP サービスに対して同一のポート番号を用いて複数の内部ネットワークのサーバ 2 に通信を要求した場合、アドレス変換機能部 25 では、アドレス変換の条件を設定できないため、指定されている GP が使用不可と判断される。

【0075】一方、ステップ S102 で、上記サービスのサービス種別とサーバ識別情報との対が、既に上記サービス情報に登録済みの場合、HGW1 は、上記サービス情報を参照し、該当する上記サービスのサービス有効期間を再設定する（ステップ S103）。このサービス有効期間を再設定は、予め設定されたサービス種別毎の公開有効期間に初期化されてもいいし、新たに上記公開有効期間を設定してもかまわない。次に、HGW1 は、上記サービスの状態が変更されている場合、状態変更処理を行う（ステップ S104）。このステップ S104 の詳細については、後述する。次に、HGW1 は、上記サービス情報を参照し、上記サービスに対する LA あるいは LP が変更されているか否かを判断し（ステップ S105）、変更されていない場合、フローを終了する。ステップ S105 で、上記サービスの LA あるいは LP が変更されていると判断された場合、HGW1 は、上記サービスに対して、上記サービス情報に示されているサービスアドレスの LA あるいは LP を更新する（ステップ S106）。その後、HGW1 は、上記サービスに対する上記サービス情報の現在の公開先が指定されているか否かを判断し（ステップ S107）、指定されている場合、スイッチ部 20 に設定されている通信路を抹消し（ステップ S108）、前述のステップ S116 に進む。一方、ステップ S107 で、現在の公開先が指定されていない場合、HGW1 は、フローを終了する。

【0076】次に、前述したステップ S104 についての詳細動作を説明する。なお、図 5 は、ステップ S104 のサブルーチンを示している。図 5 において、HGW1 は、上記サービス情報を参照し、上記サービス登録によって状態が変化するか否かを判断する（ステップ S201）。HGW1 は、上記サービス登録によって状態が変化しない場合、フローを終了する。一方、上記状態が上記サービス登録によって使用可→使用不可あるいは使用不可→使用可に変化する場合、HGW1 は、上記状態が使用不可→使用可に変化するか否かを判断する（ステップ S202）。上記サービス登録によって状態が使用不可→使用可に変化する場合、HGW1 は、上記サービス情報の上記サービスの状態を「使用可」に更新する

（ステップ S203）。そして、HGW1 は、上記サービスに対して、上記サービス詳細公開ポリシーの公開条件が「認証なし」か否か（ステップ S204）と、公開先相手が指定されているか否かとを判断する（ステップ

S 205)。公開条件が「認証なし」で、公開先相手が指定されている場合、HGW1は、上記指定されている公開先相手を上記サービス情報の現在の公開先に設定する(ステップS 206)。その後、HGW1は、上記サービスに対して、上記サービス詳細公開ポリシーの公開ポートが「指定なし」か否かを判断する(ステップS 207)。そして、HGW1は、上記公開ポートが「指定なし」の場合、空ポート番号(GP)を取得した後(ステップS 208)ステップS 211に進み、上記公開ポートが指定されている場合、指定されているポート(GP)が使用可か否かを判断する(ステップS 209)。そして、HGW1は、指定されているGPが使用可の場合、そのGPを取得する(ステップS 210)。その後、HGW1は、公開先相手に外部端末3のIAが指定されている場合、上記サービスに対して、公開先のアドレス情報(外部端末3のIAおよびIP)と内部アドレス情報(LAおよびLP)と、外部公開用アドレス情報(HGW1のGAおよび上記GP)とを取得してIPフィルタ機能部23およびアドレス変換機能部25を設定することによりスイッチ部20の通信路を設定し(ステップS 211)、フローを終了する。なお、HGW1は、公開先相手に「全て公開」が指定されている場合、上記サービスに対して、内部アドレス情報(LAおよびLP)と、外部公開用アドレス情報(HGW1のGAおよび上記GP)とを取得してIPフィルタ機能部23およびアドレス変換機能部25を設定することによりスイッチ部20の通信路を設定する。このようにして、サービスの状態が、「使用不可」→「使用可」に変更された場合、スイッチ部20の通信路が設定される。一方、ステップS 209で、指定されているGPが使用不可の場合、HGW1は、上記サービス情報を参照して、上記サービスの状態を「使用不可」に設定し(ステップS 212)、フローを終了する。

【0077】一方、ステップS 202で上記サービス登録によって状態が使用可→使用不可に変化する場合、HGW1は、上記サービス情報を参照して、該当するサービスの状態を「使用不可」に設定する(ステップS 213)。その後、HGW1は、上記サービスに対して、スイッチ部20で設定されていた通信路(ステップS 214)および上記サービス情報の現在の公開先を抹消し(ステップS 215)、フローを終了する。したがって、サービスの状態が、「使用可」→「使用不可」に変更された場合、スイッチ部20の通信路が遮断される。

【0078】次に、上記サービス詳細公開ポリシーの公開条件が「認証後公開」となっているサービス(以下、認証サービスとする)に対して、スイッチ部20の通信路が外部から設定される動作について説明する。なお、図6は、HGW1が、認証サービスに対して、上記通信路が外部から設定される動作を示すフローチャートである。

【0079】図6において、HGW1は、外部端末3からHGW1の専用GP(典型的には、ポート80)を介して、通信路設定要求を受信する(ステップS 301)。次に、HGW1は、上記通信路設定要求を送信した外部端末3に対して、ユーザ認証を要求する(ステップS 302)。これは、典型的には、ユーザ名とパスワードの入力を要求することによってユーザ認証を要求する。そして、HGW1は、上記ユーザ認証要求に対する入力結果を上記外部端末3から受信し、認証登録部32で上記入力結果が予め認証登録部32に記憶されているユーザ登録と一致するか否かを判断する(ステップS 303)。上記入力結果が上記ユーザ登録と一致しない場合、HGW1はフローを終了する。一方、上記入力結果が上記ユーザ登録と一致する場合、HGW1は、上記ユーザに対して、前述したサービス詳細公開ポリシーに公開先相手として許可されており、かつ前述したサービス情報の状態が使用可である認証サービスの一覧を上記外部端末3に送信する(ステップS 304)。次に、HGW1は、上記一覧からユーザによって選択された認証サービスおよびその認証サービスを提供するサーバの選択結果を受信する(ステップS 305)。

【0080】その後、HGW1は、上記認証サービスに対して、上記サービス情報の状態は使用可か否か(ステップS 306)、ステップS 303と同様のユーザ認証の再確認(ステップS 307)、および上記ユーザが上記サービス詳細公開ポリシーの公開先相手として許可されているか否か(ステップS 308)を再確認する。これは、上記一覧から選択されなかった場合等を想定したセキュリティ対策である。なお、ステップS 307のユーザパスワード確認は、ステップS 303とは異なった上記認証サービス固有のパスワードを確認に使用してもかまわない。なお、HGW1は、ステップS 306～S 308で不可と判定した場合、全てフローを終了する。

【0081】ステップS 308で、上記ユーザが公開先相手として許可されている場合、HGW1は、上記認証サービスに対して、上記サービス詳細公開ポリシーの公開ポートが「指定なし」か否かを判断する(ステップS 309)。そして、HGW1は、上記公開ポートが「指定なし」の場合、空ポート番号(GP)を取得した後(ステップS 310)ステップS 313に進む。一方、上記公開ポートが指定されている場合、HGW1は、指定されているポート(GP)が使用可か否かを判断する(ステップS 311)。そして、HGW1は、指定されているGPが使用可の場合、そのGPを取得した後(ステップS 312)、上記認証サービスに対する内部アドレス情報(LAおよびLP)、外部公開用アドレス情報(HGW1のGAおよび上記GP)および外部端末3のアドレス情報(外部端末3のIAおよびIP)を取得してIPフィルタ機能部23およびアドレス変換機能部25を設定することによりスイッチ部20の通信路を一時

的に設定する(ステップS313)。そして、HGW1は、上記サービス情報の現在の公開先に上記ユーザ名と公開先のアドレス情報(外部端末3のIAおよびIP)とを追加する(S314)。なお、上記外部端末3のアドレス情報は、上記通信路設定要求データの送信元IPアドレスを取得してもいいし、上記ユーザによって新たに指定されてもかまわない。

【0082】このように、「認証後公開」のサービスは、許可されたユーザのみ接続が可能であり、ユーザ認証後は、上記ユーザが現在使用している外部端末3のアドレス情報に基づいて、スイッチ部20の通信路が設定される。その後、HGW1は、外部端末3に対して、通信路を設定したサーバ2との通信に使用するポート番号を通知し(ステップS315)、フローを終了する。一方、ステップS311で、指定されているGPが使用不可の場合、上記サービス情報を参照して、上記認証サービスの状態を「使用不可」に設定し(ステップS316)、外部端末3に上記サービスが使用不可であることを通知した後、フローを終了する。

【0083】ここで、上述のように上記ユーザに対して設定された通信路は、上記サービスに対して一時的に通信路を設定される。HGW1の通信路設定機能部34は、上記通信路のデータ通信量を監視し予め設定された期間内にデータ通信がない場合、上記通信路を抹消する。なお、上記データ通信量の監視は、スイッチ部20で行い、その結果を通信路設定機能部34に通知してもかまわない。さらに、HGW1は、上記サービスの接続が終了したことを上記ユーザが使用する外部端末3あるいはサーバ2から通知させ、その通知を受信することによっても上記通信路を抹消する。

【0084】次に、HGW1で行われるサービス有効期限管理について説明する。なお、図7は、HGW1が行うサービス有効期限管理の動作を示すフローチャートである。以下、図7を参照して、サービス有効期限管理について説明する。

【0085】図7において、HGW1は、上記サービス情報に登録されているそれぞれのサービスに対してサービス有効期間が有効か否かを判断する(ステップS401)。サービス有効期間が有効である場合、HGW1は、フローを終了し、サービス有効期間のチェックを継続する。一方、サービス有効期間が終了しているサービスがある場合、HGW1は、そのサービスに対して上記サービス情報の状態を「使用不可」に設定する(ステップS402)。そして、HGW1は、上記サービスに対して、スイッチ部20に設けられている通信路(ステップS403)と、上記サービス情報の現在の公開先とを抹消する(ステップS404)。次に、HGW1は、上記サービスに対して、エントリ削除タイマTを起動させ(ステップS405)、予め設定されている削除猶予時間が経過するまで待機する(ステップS306)。上記

待機中に前述したサービス登録が行われ、上記サービスに対してサービス有効期間の再設定が行われた場合、HGW1は、フローを終了する(ステップS407)。このように、上記削除猶予時間を設けることにより、再度状態が使用可になった場合、外部からは同じポート番号(GP)で接続することが可能である。一方、上記エントリ削除タイマTが上記削除猶予時間を経過した場合、HGW1は、上記サービスを上記サービス情報のエントリから削除し(ステップS408)、フローを終了する。したがって、サービス有効期間が無効になった場合、上記サービスは、上記削除猶予時間を経て上記サービス情報から抹消される。

【0086】次に、前述のように設定された通信路に対して、スイッチ部20が設定される動作について説明する。まず、当該実施形態では、内部ネットワークから外部ネットワークへの通信は、動的IPマスカレードが自動的に適用され、ディレクトリ管理機能部33がスイッチ部20の通信路の設定を行わなくても通信が可能となるように、IPフィルタ機能部23およびアドレス変換機能部25が設定されている。なお、図11は、内部ネットワークから外部ネットワークへの通信を許可するためのIPフィルタ機能部23に設定されるパケットフィルタの情報を示す図である。

【0087】図11において、方向は、PHY・MAC機能部26が送信する方向を示し、「外」の場合、内部ネットワークと接続されているPHY・MAC機能部26bで受信し、外部ネットワークと接続されているPHY・MAC機能部26aから送信されるパケットであることを示している。また、「内」の場合、外部ネットワークと接続されているPHY・MAC機能部26aで受信し、内部ネットワークと接続されているPHY・MAC機能部26bから送信されるパケットであることを示している。そして、SA(ソースアドレス)とDA(デスティネーションアドレス)とは、それぞれパケットに付与されている送信元アドレスと送信先アドレスとを示している。また、SP(ソースポート)とDP(デスティネーションポート)とは、それぞれパケットに付与された送信元ポート番号と送信先ポート番号とを示している。また、ACK(Acknowledgement Flag)は、ACKをチェックするか否かを示している。なお、ACKは、接続を確立するパケットではセットされず、それ以降のパケットでセットされている。このIPフィルタ機能部23に設定されている情報は、デフォルト設定AおよびBとして予め設定されている。したがって、内部ネットワークのサーバ2からHGW1へ通信を開始するパケットを送信した場合、デフォルト設定Aによってパケットフィルタの通過が許可される。そして、外部ネットワークの外部端末3からHGW1への応答は、デフォルト設定Bによってパケットフィルタの通過が許可される。一方、外部ネットワークの外部端末



3からHGW1へ通信を開始するパケットを送信した場合、そのパケットにACKがセットされていないため、デフォルト設定Bによって通過を拒否される。すなわち、新たなパケットフィルタの設定を追加しない限り外部ネットワークから内部ネットワークに通信を開始することができない。

【0088】次に、FTPサービスを公開する場合、スイッチ部20のIPフィルタ機能部23およびアドレス変換機能部25に設定される情報について説明する。なお、図12(a)はFTPサービスの通信シーケンスを示す図であり、図12(b)はディレクトリ管理機能部33によってアドレス変換機能部25に設定されるアドレス変換テーブルを示す図であり、図12(c)はディレクトリ管理機能部33によってIPフィルタ機能部23に設定されるパケットフィルタを示す図である。以下、図12を参照して、FTPサービスの通信路設定要求が行われた場合、制御用セッションのパケットが伝送する形態について説明する。

【0089】まず、外部端末3から、ソースアドレスIA、ソースポート番号IP1、デスティネーションアドレスGAおよびデスティネーションポート番号21が付与されたパケットが送信される。次に、HGW1は、上記パケットを受信し、アドレス変換機能部25のアドレス変換テーブルの条件Cを適用することにより、デスティネーションアドレスGAおよびデスティネーションポート番号21をそれぞれFTPサーバ2のLAおよびLP21に変換する。その後、IPフィルタ機能部23は、上記パケットに対してパケットフィルタの条件Eを適用することによってフィルタリング処理を実行し、上記パケットの通過を許可する。次に、フォーワーディング機能部24によって、上記パケットは、内部ネットワークと接続されているPHY・MAC機能部26bを介してFTPサーバ2へ送信される。

【0090】そして、FTPサーバ2は、外部端末3からの上記パケットを受信した後、ソースアドレスLA、ソースポート番号21、デスティネーションアドレスIAおよびデスティネーションポート番号IP1が付与された応答パケットをHGW1へ送信する。次に、HGW1は、上記応答パケットを受信し、上記応答パケットに対してIPフィルタ機能部23のパケットフィルタのデフォルト設定Aを適用することによってフィルタリング処理を実行し、上記応答パケットの通過を許可する。その後、アドレス変換機能部25のアドレス変換テーブルの条件Dを適用することにより、ソースアドレスLAおよびソースポート番号21をそれぞれHGW1のGAおよびGP21に変換する。次に、フォーワーディング機能部24によって、上記応答パケットは、外部ネットワークと接続されているPHY・MAC機能部26aを介して外部端末3へ送信される。

【0091】また、上記FTPサービスでは、上記制御

用セッションの他に、データ用セッションが外部端末3とFTPサーバ2との間でポート番号20を用いて確立される。このデータ用セッションの確立は、FTPサーバ2から通信を開始することにより行われるため、動的IPマスカレードとデフォルトのフィルタリング設定により、ディレクトリ管理機能部33によって特別な設定が行われなくても内部ネットワークからの通信が可能となる。

【0092】なお、前述したFTPサービスによる伝送形態では、内部ネットワークから外部ネットワークへの通信は、動的IPマスカレードが自動的に適用され、ディレクトリ管理機能部33がスイッチ部20の設定を行わなくても内部からの通信が可能となるように、IPフィルタ機能部23およびアドレス変換機能部25が設定されている。しかしながら、HGW1のセキュリティをさらに高めるために、上記動的IPマスカレードやデフォルトのパケットフィルタの設定を行わなくてもかまわない。このような場合、外部ネットワークの外部端末3からFTPサーバ2にアクセスするためには、FTPサーバ2のLPに対応するアドレス変換とパケットフィルタとの一連の設定が必要となる。これは、サービス種別に応じてLPに対応する一連の設定用テンプレートを予め用意しておくことで、容易にIPフィルタ機能部23およびアドレス変換機能部25の設定を行うことができる。なお、上記設定用テンプレートがないサービス種別のサービスが登録された場合、上記設定用テンプレートをサーバ2あるいは外部ネットワークの定められたサーバから取得することによって、IPフィルタ機能部23およびアドレス変換機能部25の設定を行うことができる。

【0093】なお、当該実施形態では、内部ネットワークを1つのネットワークとして説明したが、HGW1に対して複数の内部ネットワークを接続してもかまわない。これは、スイッチ部20に第3のPHY・MAC機能部26を増設し、上記第3のPHY・MAC機能部26に外部ネットワーク公開用のサーバを有する第2の内部ネットワーク(DMZ: De Militarized Zone)を接続することにより、本発明を適用し、さらにセキュリティを向上することができる。

【0094】なお、本実施形態では、サービス状態の「使用可」から「使用不可」への状態遷移や「使用不可」から「使用可」への状態遷移、及びサービス情報の登録・削除のために、サーバからの登録情報や有効期限のタイムアウトの情報を用いるとしたが、これに限らず、HGW1がサーバに対してポートスキャンを実行し、サーバのオープンされたポートの変化に基づいてサービス状態の遷移やサービス情報の登録・削除を実行するようにしてもよい。同様に、ポートスキャンの代わりにpingを用いてもよい。

【0095】また、本実施形態では、外部ネットワーク

より内部ネットワークのサーバにアクセスする例を示したが、これに内部ネットワークのべつの機器よりアクセスしてもよい。その場合、現在の公開先に内部ネットワークの機器に対する詳細公開ポリシーを追加する、または、もうひとつ別に公開先のテーブルを持つことで実現できる。これにより、内部からアクセスした場合と外部からアクセスした場合でセキュリティの強度を変えることができ、利便性が増す。

【0096】なお、あるサーバについてサービス詳細公開ポリシーを作成する際には、宅外の、例えばそのサーバの製造元にアクセスし、そこからサービス詳細公開ポリシーの初期値を取得してもよい。これにより、そのサーバに格納されているサービス詳細公開ポリシーを、製造者はサーバ出荷後も変更することが可能となる。

【0097】このように、当該ファイアウォール装置では、外部から接続可能なユーザを限定しユーザ認証を確認した後、そのユーザが使用している外部端末のアドレス情報（IA、IP）を取得し、そのアドレス情報を基にして通信路を設定している。したがって、内部ネットワークのサービスに対して、外部からアクセス可能なユーザを限定して公開することができ、しかも、上記ユーザがサービス公開を要求する期間のみ通信路を設定することができる。また、上記ユーザが使用する外部端末を変更する、あるいはユーザが使用している外部端末のIAが変わっても同様のアクセスが可能である。また、上記ユーザは、通信路を設定する要求をするとき、アクセス可能なサービスを選択的に接続することができ、さらに、同じサービスを内部ネットワーク内で複数のサーバが有していても、上記ユーザは上記サーバを選択的に接続することができる。一方、内部ネットワークのサーバに接続可能なユーザを、そのサーバのサービス毎に設定できるため、内部ネットワークの中で同一のサービスを有する複数のサーバに対して、それぞれの異なった接続可能なユーザを設定することにより、サーバ毎のセキュリティレベルを容易に設定することができる。さらに、内部ネットワークのサーバのアドレス情報（IA、IP）が変更された場合、当該ファイアウォール装置は、上記サーバを識別する固定値を認識することにより、上記サーバと変更された上記アドレス情報とを対応させることができるため、アドレス変換時に必要なテーブルの変更を自動的に容易に処理することができる。また、当該ファイアウォール装置は、外部ネットワークに提供可能なサービスに対して有効期限を設けており、上記サービスが有効である時のみ一時的に通信路を設定し、しかも上記サービス専用の通信路であるため、さらにセキュリティの向上を実現できる。

【0098】なお、本実施形態では、登録しようとするサービスのサービス種別とサーバ識別情報との対がディレクトリ管理機能部33に未登録であった場合、図4のステップS109に示すようにサービス基本公開ポリシ

ーに基づいてサービス詳細公開ポリシーを設定するとしたが、他の方法によりサービス詳細公開ポリシーが決定されるようにしても構わない。例えば、サービス詳細公開ポリシーとしてすでに登録されている項目の中から、新たに登録しようとするサービスと同じサービス種別のものの個数を数え、その個数があるしきい値以上である場合にはそれらすでに登録されている項目に基づいてサービス詳細公開ポリシーを設定し、一方、その個数がしきい値未満である場合にはサービス基本公開ポリシーに基づいてサービス詳細公開ポリシーを設定するようにしても構わない。つまり具体的には、図4のステップS109の代わりに例えば図14に示す処理が実行されるようにしても構わない。以下、図14～図16を参照してより具体的に説明する。

【0099】今、内部ネットワークにIPがLA5であるサーバ2-4が新たに設けられたと仮定する。つまり、ディレクトリ管理機能部33に図15に示すようなサービス情報が新たに登録される場合について考える。ディレクトリ管理機能部33は、図4のステップS102においてサーバ2-4が提供するサービスが未登録であると判断すると、図14のステップS203において、すでにディレクトリ管理機能部33において管理されているサービス詳細公開ポリシーの中から、新たに登録するサービスに関連する項目を抽出する。次にディレクトリ管理機能部33はステップS204において、抽出した項目の数が3以上であるか否かを判断し、3未満である場合には図4のステップS109と同様の処理によりサービス詳細公開ポリシーを設定する。一方、ステップS204において項目の数が3以上であると判断された場合には、ステップS206において、抽出した項目の設定内容に基づいてサービス詳細公開ポリシーを設定する。以上の処理について図16を参照してより具体的に説明すると、新たに追加されるサーバ2-4のHTTPサーバの項目については、この項目とサービス種別が一致する項目が2個（図中の項目A、B）なので、このサーバ2-4のHTTPサーバの公開先相手・公開条件・公開ポートは、図9に示すサービス基本公開ポリシーに基づいて決定される。一方、サーバ2-4のFTPサーバの項目については、この項目とサービス種別が一致する項目が3個（図中の項目C～E）なので、このサーバ2-4のFTPサーバの公開先相手・公開条件・公開ポートは、項目C～Eの設定内容に基づいて決定される。ここでは、項目C～Eに共通の設定がサーバ2-4のFTPサーバの設定に反映される。

【0100】なお、抽出した項目の設定内容に基づいてサービス詳細公開ポリシーを設定する具体的な方法については種々の方法が考えられる。例えば上記の説明では、サービス詳細公開ポリシーを作成する際、すでに登録されている項目の設定内容の論理積を取ることにより新たなサービスの設定内容を決定したが、これに限ら

ず、例えばすでに登録されている項目の設定内容の論理和や多数決を取ることににより新たなサービスの設定内容を決定しても構わない。これらまたは他の種々の設定方法については下記の種々の実施形態の説明によっても示唆される。

【0101】(第2の実施形態)図17に、本発明の第2の実施形態に係る通信装置100の構成を示す。通信装置100は、制御メニュー構成部110と、ディレトリ管理機能部120と、制限項目管理部130とを備える。制御メニュー構成部110は、制御メニュー作成要求受信部111と、制御メニュー作成部112と、制御メニュー送信部113とを含む。ディレトリ管理機能部120は、ネットワーク構成要素検出部121と、ネットワーク情報取得部122と、ネットワーク情報格納部123とを含む。制限項目管理部130は、制限項目作成部131と、初期制限項目格納部132と、個別制限項目格納部133と、入力部134とを含む。

【0102】通信装置100は、ユーザがネットワークを介して制御端末から被制御端末を制御する際に、予め設定された制限項目に基づいて、その制御を許可したり、あるいは制御を一部制限したり、あるいは制御を禁止したりする機能を有する。より具体的に説明すると、例えば、太郎さんの宅内に設けられたネットワーク(IEEE1394バス)に接続されたビデオを被制御端末としてネットワークを介して制御するとき、通信装置100は、制御を行うのが太郎さんであれば、宅内のネットワークに接続された制御用端末からでも、インターネットに接続された制御用端末としての携帯電話からでもビデオを制御できるようにし、一方、制御を行うのが太郎さんの娘の花子さんであれば、宅内のネットワークに接続された制御用端末からはビデオを制御できるが、携帯電話からは制御できないようにするというように、条件に応じて被制御端末の制御を制限する。

【0103】図17は、一例として、宅外ネットワークとしてのインターネット160に接続された例えば携帯電話等の制御端末141から、宅内ネットワークとしてのIEEE1394バス170に接続された、それぞれAV/Cコマンドを実装した例えばビデオやチューナ等の被制御端末151~153を制御する場合の構成を示している。

【0104】以下、通信装置100の動作を説明する。ディレトリ管理機能部120は、ネットワークに接続されている機器に関する情報を要素情報として管理している。図18に、ネットワーク情報格納部123で管理される要素情報の一例を示す。図18において、GUIDとは、機器毎にユニークに与えられている64ビットの識別子である。また、機器カテゴリーとは、機器の種類を示すものである。また、サービス情報とは、機器がネットワークに対して提供できるサービスを示すものである。また、所属ネットワークとは、機器が属するネッ

トワークを示すものである。すなわち、図18に示す要素情報は、IEEE1394バスには、機器として、ネットワークを介して「電源」「録画」「再生」「早送り」「巻き戻し」「停止」の制御が可能な2台のビデオと、ネットワークを介して「電源」「選局」の制御が可能な1台のチューナが接続されていることを示している。

【0105】ディレトリ管理機能部120は、通信装置100に接続されるネットワークに新たな機器が接続されたとき、それを検知して要素情報を更新する機能を有する。以下、この機能について具体的な例で説明する。図19に、機器152、153がすでにIEEE1394バス170に接続されている状態で、機器151がIEEE1394バス170に新たに接続されたときの動作シーケンスを示す。なお、他の実施形態も含めた以下の説明において、例えば図17における被制御端末151等を、単に機器151等として説明しているが、これは、ネットワークに接続されている機器が制御端末となるか被制御端末となるかは、予め決められている必要はなく、例えば機器がPC等であれば、状況に応じて制御端末として利用されたり被制御端末として利用されたりする。よって、制御の主体と客体を意識しない段階では単に機器151等としている。IEEE1394バス170に新たな機器(ここでは機器151)が接続されるとバスリセットが発生する。ネットワーク構成要素検出部121は、このバスリセットを検出し、バスリセットが発生したことをネットワーク情報取得部122に通知する。ネットワーク情報取得部122は、この通知を受けると、IEEE1394バス170に接続されている機器のGUIDを取得する。ネットワーク情報取得部122は、取得したGUIDをネットワーク情報格納部123に通知する。

【0106】ネットワーク情報格納部123は、すでに格納されている要素情報を参照して、ネットワーク情報取得部122から通知されたGUIDと、バスリセット発生前に接続されていた機器のGUIDとを比較する。その結果、新たに機器151のGUIDが増えていることが確認されるので、ネットワーク情報格納部123は、要素情報を更新すべく、ネットワーク情報取得部122に対し、この新たに接続された機器151が提供するサービス情報と、機器カテゴリーとを取得するように要求する。ネットワーク情報取得部122は、AV/Cコマンドを用いて、機器151が提供するサービス情報および機器カテゴリーを示す情報を取得する。

【0107】ネットワーク情報取得部122は、取得したビデオA151のサービス情報および機器カテゴリーを示す情報を、ネットワーク情報格納部123に通知する。ネットワーク情報格納部123は、通知された情報を要素情報に登録することにより、要素情報を更新する。

【0108】ユーザが制御端末から被制御端末を制御するには、まず、通信装置100に対して、被制御端末を制御するための制御メニューを要求する。制御メニュー構成部110は、制御端末からの要求に基づいて、制御メニューを構成して制御端末へ送る。図20に、制御端末に送られた制御メニューの画面表示の一例を示す。ユーザは、この制御メニューに基づいて、例えばビデオA151の録画を開始するなど、制御端末から被制御端末を制御することができる。制限項目管理部130には、種々の条件毎に被制御端末の制御を許可するか禁止するかを規定するための制限項目が、予め設定されて登録されている。図21に、制限項目管理部130において管理されている制限項目の一例を示す。この図21の例では、被制御端末と、制御を行うユーザと、制御端末のネットワークと、被制御端末のネットワークとの組合せに応じて特定される制御条件毎に、被制御端末の制御を許可するか禁止するかを示す制限情報が設定されている。図21の例によれば、例えば、「IEEE1394」に接続された、GUIDが「0x0123456789012345」である被制御端末に対して、「太郎」が、「インターネット」に接続された制御端末から制御を行う場合には、制限情報として「アクセス許可(1)」が設定されているため、制御が許可される。一方、「IEEE1394」に接続された、GUIDが「0x0123456789012345」である被制御端末に対して、「花子」が、「インターネット」に接続された制御端末から制御を行う場合には、制限情報として「アクセス不可(0)」が設定されているため、制御が禁止される。制御端末へ送られる制御メニューは、この制限項目管理部130が管理している制限項目に基づいて作成され、制御端末から制御することのできる制御内容のみで構成される。これにより、制限項目管理部130が管理している制限項目に応じて、制御端末からの被制御端末の制御が制限されることになる。

【0109】以下、ユーザが制御端末で制御メニューを取得する際の処理について具体的な例で説明する。図23に、制御端末141で制御メニューを取得するときの動作シーケンスを示す。なお、ここでは、機器151がIEEE1394バス170に新たに接続されてから一番最初に制御メニューが要求されたという状況を仮定して説明を行う。ユーザは、制御メニューを取得するために、制御端末141を操作して、通信装置100に対して制御メニュー要求を発行する。制御メニュー作成要求受信部111は、この要求を受け、制御メニュー要求を発行したユーザのユーザIDおよび制御端末141が接続されているネットワークを識別する。ここで、ユーザ識別のための情報取得は、制御端末141が制御メニュー要求を発行するまでに行われていればよいが、セキュリティ上、制御端末141と通信装置100とのコネクションが確立した後に制御端末141からユーザIDお

よびパスワードが送付されてユーザ認証が行われるのが望ましい。

【0110】制御メニュー作成要求受信部111は、ユーザIDおよび制御端末のネットワーク情報を制御メニュー作成部112に送り、制御メニューの作成を要求する。要求を受けた制御メニュー作成部112は、まず、ネットワーク情報格納部123に対して、現在IEEE1394バス170に接続されている機器に関する情報である要素情報を要求する。ここで要求される要素情報は、機器のGUIDと、機器カテゴリと、サービス情報と、そのネットワークの種類とからなる。ネットワーク情報格納部123は、前述のように管理している要素情報に基づいて、制御メニュー作成部112に対して要素情報を通知する。

【0111】次に、制御メニュー作成部112は、制御メニュー作成要求受信部111から受け取ったユーザIDおよび制御端末のネットワーク情報と、ネットワーク情報格納部123から受け取った要素情報とを制限項目作成部131に通知し、これらの情報に応じた制限項目を要求する。

【0112】制限項目作成部131は、制御メニュー作成部112からの制限項目要求を受けると、制御メニュー作成部112から通知された「GUID」と、「ユーザID」と、「被制御端末のネットワーク」と、「制御端末のネットワーク」とを個別制限項目格納部133に送信する。個別制限項目格納部133では、前述した図21に示す制限項目が予め登録されており、制限項目作成部131から送信された情報をもとに、それに合致する制限情報を検索し、制限項目作成部131に通知する。例えば、要素情報に、GUIDが「0x0123456789012345」である機器に関する情報が含まれている場合、この機器が現在接続されているネットワーク「IEEE1394」と、この機器を制御しようとするユーザのID「太郎」と、制御端末が接続されているネットワーク「インターネット」との組合せに対して設定されている制限情報を検索する。検索の結果、制限情報として「アクセス許可(1)」が設定されていることが分かる。要素情報に含まれる他のGUIDで示される機器についても同様の検索を行う。個別制限項目格納部133は、こうして得られた制限情報を制限項目作成部131に通知する。

【0113】なお、図21に示すのは、新たに接続された機器151に関する個別制限項目(図21に新項目A、Bで示す)が後述する処理等によって新たに登録された後の内容を示している。ここでは、これら新項目A、Bが、まだ登録されていない状態を仮定して説明を行っているため、この段階における個別制限項目の内容は、図22に示す内容となっている。

【0114】一方、個別制限項目格納部133における検索の結果、その条件に合致する制限項目が登録されて

いない場合がある。ネットワークに被制御端末として新たな機器を接続した場合である。また、場合によっては、機器の接続先のネットワークを変更した場合などにもこのような状況が起こり得る。また、太郎に対する登録はされていても、花子に対する登録がまだされていないような場合などにもこのような状況が生じ得る。このような状況が生じたとき、従来では、この新たに接続した機器に対する制限項目をユーザがその都度設定する必要があり、ネットワークに対して十分な知識を持たない者（例えば家族の誰かなど）が勝手に機器をネットワークに接続した場合には、誤った設定が行われて宅外から無制限にアクセスされる可能性があるという問題があることについては前述した通りである。

【0115】本実施形態では、個別制限項目格納部133における検索の結果、その条件に合致する制限項目が登録されていなかった場合、初期制限項目格納部132に予め設定しておいた初期制限項目に基づいて条件に合致した制限情報を取得することにより、ユーザによる設定を必要とすることなく好ましい制限情報が自動的に設定される。より具体的に説明すると、制限項目作成部131は、初期制限項目格納部132に対し、登録がされていなかった条件について、「ユーザID」と、「制御端末のネットワーク」と、「被制御端末のネットワーク」とを送信する。初期制限項目格納部132は、初期制限項目の中から、この条件に一致する制限情報を検索し、制限項目作成部131に対して通知する。図24に、初期制限項目格納部132に登録されている初期制限項目の一例を示す。図24において、例えば、「IEEE1394」に新たな機器が接続され、その後「太郎」が「インターネット」に接続された制御端末から制御メニューを要求した場合、この条件に応じて初期制限項目を検索した結果、この条件に合致した制限情報として「アクセス許可(1)」が設定されているので、これを制限項目作成部131に対して通知する。

【0116】制限項目作成部131は、初期制限項目格納部133から通知された制限情報に基づいて、個別制限項目格納部133に新たな制限項目を登録する。例えば、IEEE1394バス170にGUIDが0x0123456789012345である被制御端末151が新たに接続された後に、太郎がインターネット160に接続される制御端末141から制御メニューを要求すると、この条件に合致する初期制限項目には「アクセス許可(1)」が設定されているので、個別制限項目格納部133に、新たな制限項目として、GUID「0x0123456789012345」、ユーザID「太郎」、制御端末のネットワーク「インターネット」、被制御端末のネットワーク「IEEE1394」からなる制御条件に対して制限情報「アクセス許可(1)」を対応付けた制限項目（図21に示す新項目A）を登録する。

【0117】制限項目作成部131は、以上の処理により条件に応じた制限情報を取得し、制御メニュー作成部112に対して制限項目を通知する。制御メニュー作成部112は、ネットワーク情報格納部123より通知された被制御端末のネットワーク情報、サービス情報および機器カテゴリーと、制限項目作成部131より通知された制限項目に基づいて制御メニューを作成する。制御メニューは、制御端末141で実行可能なアプリケーションの形式でもよいが、好ましくは、HTMLで記述されたソースであることが望ましい。この場合、制御端末141はHTMLブラウザを装備していれば、機器の制御を行うことが可能となる。さらに、制御メニューで表示される項目と制御コマンドがCGIなどで関連付けられていることが望ましい。

【0118】制御メニュー作成部112は、作成した制御メニューを制御メニュー送信部113に送信する。制御メニュー送信部113は、受け取った制御メニューを制御端末（ここでは制御端末141）に送信する。制御端末141は、制御メニューをブラウザに表示し、ユーザは制御メニューに基づいて操作を行い、被制御端末151～153の制御を行う。

【0119】図25に示すフローチャートを参照して、制限項目作成部131の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部123に図18に示す要素情報が格納されており、初期制限項目格納部132に図24に示す初期制限項目が格納されている状態において、図21に示す個別制限項目において、GUIDが「0x0123456789012345」である被制御端末151に関する制限項目（図中の新項目A、B）が未登録である状況、つまり図22に示す制限項目が登録されている状況、を想定して説明する。

【0120】制限項目作成部131は、ステップS901で、制御メニュー作成部112より、制限情報を作成する条件として、「GUID」と「ユーザID」と「制御端末のネットワーク情報」と「被制御端末のネットワーク情報」を受け取る。ここで受け取る項目は以下の通りである。

【0121】GUID=0x0123456789012345

ユーザID=太郎

被制御端末のネットワーク情報=IEEE1394（以下、単に宅内と称す）

制御端末のネットワーク情報=インターネット（以下、単に宅外と称す）

GUID=0x0123456789123456

ユーザID=太郎

被制御端末のネットワーク情報=宅内

制御端末のネットワーク情報=宅外

GUID=0x0123456789234567

ユーザID=太郎

被制御端末のネットワーク情報=宅内

制御端末のネットワーク情報=宅外

【0122】ステップS902で、上記の条件をもとに、個別制限項目格納部133に個別制限項目を送るよう要求する。ステップS903で、上記の条件に対する制限情報を受け取る。ここで受け取る項目は以下の通りである。

【0123】GUID=0x0123456789012345

ユーザID=太郎、

被制御端末のネットワーク情報=宅内

制御端末のネットワーク情報=宅外

制限情報=

GUID=0x0123456789123456

ユーザID=太郎

被制御端末のネットワーク情報=宅内

制御端末のネットワーク情報=宅外

制限情報=アクセス許可

GUID=0x0123456789234567

ユーザID=太郎、

被制御端末のネットワーク情報=宅内

制御端末のネットワーク情報=宅外

制限情報=アクセス許可

【0124】ステップS904で、制限情報が存在しない条件が存在するか否かを確認する。存在すればステップS905に進み、存在しなければステップS908に進む。ここでは、GUID=0x0123456789012345の条件が、制限情報が存在しない条件にあたる。

【0125】ステップS905で、制限情報が存在しない条件について、初期制限項目格納部132に対して、この条件に対応する制限項目を通知するように要求する。ステップS906で、条件に一致する制限情報を受け取る。ここで受け取る項目は以下の通りである。

【0126】ユーザID=太郎、

被制御端末のネットワーク情報=宅内

制御端末のネットワーク情報=宅外

制限情報=アクセス許可

【0127】ステップS907で、前述のステップS906で受け取った制限項目を個別制限項目格納部133に登録する。この結果、図21に新項目Aで示した個別制限項目が新たに登録される。ステップS908で、制御条件と制限情報とを対応付けて制御メニュー作成部112に通知する。

【0128】この後、制御メニュー作成部112で作成された制御メニューは、制御メニュー送信部113を通じて制御端末141に送信される。制御メニュー作成部112は、図18に示されるサービス情報のうち、図21に示される個別制限項目でアクセスが許可されている

ものだけを選択し、制御メニューとする。よって、図20に示すように、ユーザ太郎が操作する制御端末141には、ビデオA151、ビデオB152、およびチューナ153の制御メニューが表示される。

【0129】一方、仮に、制御メニューを要求したユーザが花子である場合、上記と同様の処理によって図21に示す新項目Bが新たに登録され、制御メニュー作成部112は、図18に示されるサービス情報のうち、図21に示される個別制限項目でアクセスが許可されているものだけを選択し、制御メニューとするのであるが、ユーザ花子についてはすべての制限項目で、インターネット160を通じたアクセスが不可に設定されているため、図26に示すように、ユーザ花子が操作する制御端末141には、制御可能な制御項目は表示されない。

【0130】なお、個別制限項目格納部133に格納されている個別制限項目は、入力部134よりユーザが設定することができる。これは、制限項目作成部131で作成されて登録された制限項目についても同様である。また、初期制限項目格納部132に格納されている初期制限項目についても、入力部134よりユーザが設定することができる。

【0131】なお、本実施形態では、宅外からのアクセスとして、インターネット160に接続されている制御端末141より制御メニューを要求したが、宅外ネットワークはインターネット以外でもよく、また、宅内のIEEE1394バス170またはその他のネットワークに接続されている制御端末より制御メニューを要求し、被制御装置を制御しても構わない。

【0132】また、本実施形態では、ユーザIDとして「太郎」を例にあげたが、これはユーザを識別するIDの例であり、ユーザに合わせて設定してもよい。また、ユーザに関する条件として、「太郎」や「花子」といった個人を対象としたユーザIDを用いて説明したが、ユーザの属性、例えばネットワーク管理者、家族、ゲストなどで分類した条件を用いても構わない。

【0133】また、本実施形態では、被制御端末が接続されるネットワークとしてIEEE1394バス170、制御端末が接続されるネットワークとしてインターネット160を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、ECHONETやBluetoothなどが挙げられる。

【0134】また、本実施形態では、2つのネットワークが通信装置100に接続される例を示したが、これに限らず、通信装置100に接続されるネットワークの数は1つまたは3以上であっても構わない。

【0135】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、2つの機器が連携して提供されるサービス、例え

ば、ビデオのダビングや通信路設定などであっても構わない。

【0136】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、機器のカテゴリーや、サービス情報や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【0137】また、本実施形態では、被制御端末として、ビデオA、ビデオBおよびチューナを例に挙げたが、チューナが通信装置を通じてビデオAを制御するなど、これらの機器が制御端末となって他の被制御機器を

制御しても構わない。

【0138】また、本実施形態では、機器カテゴリーの分類項目としてビデオやチューナを使用した、AV機器や空調機器など他の分類を行っても構わない。

【0139】また、本実施形態では、ネットワーク情報格納部123に格納されている要素情報に基づいて制御の制限を行ったが、それに代えて、制御メニュー作成部112から要素情報を要求された時点で、ネットワーク情報取得部122が要素情報を取得して制御メニュー作成部112に通知するようにしても構わない。要素情報を格納しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、要素情報を必要に応じて取得する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【0140】また、本実施形態では、制御メニューを作成する際に新たな条件に合致する制限項目の作成を行ったが、これに限らず、それ以前のタイミングで作成しても構わない。例えば、新たな構成要素が検出された段階でこれを行ってもよい。この場合、制御メニューを作成する際に作成する場合と比較し、ユーザが制御メニューを要求してから、制御メニューを受け取るまでの時間が短くなるという利点がある。

【0141】以上のように、第2の実施形態によれば、対応する個別制限項目が存在しない場合、初期制限項目を用いてアクセス制限を行うため、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【0142】また、制御機器が接続されるネットワークの種類に応じてアクセス制限を設定しているため、例えばインターネットのように不特定多数が利用するネットワークであればアクセスを不可とし、IEEE1394バスのような宅内のネットワークであればアクセスを許可するというように、利便性と安全性を両立した制限が可能となる。

【0143】(第3の実施形態)以下、本発明の第3の実施形態に係る通信装置について、図面を参照しながら説明する。図27に、本実施形態に係る通信装置1000と、それに接続されるネットワークおよび制御端末、

被制御端末とを示す。図27において、通信装置1000は、制御メニュー構成部110と、ディレクトリ管理機能部120と、制限項目管理部1030を含む。制御メニュー構成部110は、制御メニュー作成要求受信部111と、制御メニュー作成部112と、制御メニュー送信部113を含む。ディレクトリ管理機能部120は、ネットワーク構成要素検出部121と、ネットワーク情報取得部122と、ネットワーク情報格納部123を含む。制限項目管理部1030は、制限項目作成部1031と、個別制限項目格納部133と、入力部134を含む。通信装置1000は、インターネット160と、IEEE1394バス170に接続され、それらネットワークには、それぞれ制御端末141(例えば、携帯電話)およびAV/Cコマンドを実装した被制御端末151、152、1054(例えば、ビデオA、ビデオB、ビデオC)が接続される。なお、図27において、図17と同一の構成には同一の参照符号を付し、その説明を省略する。

【0144】以下、通信装置1000の動作を、特に第2の実施形態に係る通信装置1000との相違点を中心に説明する。ここでは、例として、機器151が新たに接続され、機器151、152、1054をユーザ(太郎)がインターネット160に接続された機器141から制御するために制御メニューを要求する場合について説明を行う。

【0145】図28に、機器151がIEEE1394バス170に接続されたときの動作シーケンスを示す。図28に示すように、第2の実施形態と同様の動作により、ネットワーク情報格納部123に要素情報が更新され登録される。図29に、ネットワーク情報格納部123に格納される要素情報の一例を示す。なお、図29に示す要素情報には、図18に示した「被制御端末のネットワーク」の情報が含まれていないが、これは、制限情報を設定する制限項目の条件として「被制御端末のネットワーク」についての情報が含まれないためである。

【0146】制御メニュー構成部110は、第2の実施形態と同様に、制御端末141からの要求に応じて制御メニューを作成する。このとき、制限項目管理部1030に対して、制限項目を要求する。制限項目管理部1030では、制御メニュー作成部112から通知される条件に応じた制限項目を制御メニュー作成部112に対して返すのであるが、第2の実施形態とは異なり、初期制限項目格納部133に条件に合致した制限項目が存在しなかった場合には、すでに個別制限項目格納部133に格納されている制限項目に基づいて、この制限項目がない条件に対する好ましい制限情報を自動的に判断して決定する。以下、その具体的な動作について説明する。

【0147】図30に、インターネットに接続された携帯電話141を使用して、ユーザIDとして太郎で登録

10

20

30

40

50

されているユーザが被制御端末 151 を制御するための制御メニューを取得する際の動作シーケンスを示す。制御端末 141 で制御メニューを要求してから制限項目作成部 1031 に制限項目要求が発行されるまでの動作については、第 2 の実施形態と同様であるので説明を省略する。

【0148】制限項目作成部 1031 は、受け取った条件を個別制限項目格納部 133 に送り、制限項目の発行を要求する。個別制限項目格納部 133 は、受け取った条件に合致する制限情報を検索して制限項目作成部 1031 に通知する。図 31 に、個別制限項目格納部 133 に格納される制限項目の一例を示す。

【0149】なお、図 31 に示すのは、新たに接続された機器 151 に関する個別制限項目（図 31 に新項目 A、B で示す）が後述する処理によって新たに登録された後の内容を示している。ここでは、これら新項目 A、B が、まだ登録されていない状態を仮定して説明を行っている。

【0150】ここで、被制御端末 151 は、新たに IEEE 1394 バス 170 に追加された機器であるため、個別制限項目格納部 133 には被制御端末 151 の GUID は登録されていない。制限項目作成部 1031 は、GUID の一致する制限項目が個別制限項目格納部 133 に登録されていなかった場合、他の機器に適用するために登録されている制限項目の中から、この条件と「ユーザ ID」、「機器カテゴリ」、および「制御端末のネットワーク情報」が一致する制限項目の検索を個別制限項目格納部 133 に対して要求する。個別制限項目格納部 133 は、この要求を受けて制限情報を検索し、その結果を、制限項目作成部 1031 に通知する。制限項目作成部 1031 は、これらの制限情報を元に、登録されていない条件に対する制限情報を決定する。具体的には、制限情報のアクセス許可を 1、アクセス不可を 0 とし、取得した制限情報で論理積をとることにより決定する。このように論理積を取ることで、設定されたすべての制限情報がアクセス許可でなければ、新たに接続された機器およびサービスもアクセス可能とはならず、不用意にアクセスを許可することがない。

【0151】こうして新たに作成された制限項目は、第 2 の実施形態と同様に個別制限項目格納部 133 に登録される。制限項目作成部 1031 は、要求された制限項目を制御メニュー作成部 112 に通知し、制御メニュー作成部 112 は、通知に基づいて制御メニューを作成する。この制御メニューは、制御メニュー送信部 113 を通じて制御端末 141 に送信される。制御端末 141 は、制御メニューをブラウザで表示し、ユーザは制御メニューに基づいて制御端末 141 を操作して被制御端末 151 の操作を行う。

【0152】図 32 に示すフローチャートを参照して、制限項目作成部 1031 の動作を説明する。以下では、

説明を分かり易くするために、具体例として、ネットワーク情報格納部 123 に図 29 に示す要素情報が格納されており、図 31 に示す個別制限項目において、GUID が「0x0123456789012345」である被制御端末 151 に関する制限項目（図中の新項目 A、B）が未登録である状況を想定して説明する。ただし、図 32 において、図 25 に示すフローと同一の処理ステップについては同一の参照符号を付し、説明を省略する。

【0153】制限項目作成部 1031 は、制御メニュー作成部 112 から受け取った条件を個別制限項目格納部 133 に通知し、条件に応じた制限情報を個別制限項目格納部 133 より取得する。ここで取得する項目は以下の通りである。

【0154】GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

機器カテゴリ=ビデオ

制限情報=

GUID=0x0123456789123456

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

機器カテゴリ=ビデオ

制限情報=アクセス許可

GUID=0x0123456789234567

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

機器カテゴリ=ビデオ

制限情報=アクセス許可

【0155】ステップ S904 で、制限情報が存在しない条件があるか確認する。存在すればステップ S1609 に進み、存在しなければステップ S908 に進む。ここでは、GUID=0x0123456789012345 に関する条件がこれにあたる。ステップ S1609 で、個別制限項目格納部 133 に対して、制限情報が存在しない条件について、GUID 以外の条件に合致する制限項目を通知するように要求する。ステップ S1610 で、前のステップ S1609 で要求した制限項目を受け取る。ここで受け取る項目は以下の通りである。

【0156】ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

機器カテゴリ=ビデオ

制限項目=アクセス許可

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

機器カテゴリ=ビデオ

制限項目=アクセス許可

【0157】ステップ S1611 で、これら制限項目の制限情報に対して論理積を取り、それをこの制限項目が



登録されていない条件に対する制限情報とする。こうして作成される制限項目は以下の通りである。

【0158】GUID=0x0123456789012345

ユーザID=太郎

制御端末のネットワーク情報=インターネット

機器カテゴリー=ビデオ

制限項目=アクセス許可

【0159】ステップS907で、新たに作成した制限項目を個別制限項目格納部133に登録する。この結果、図31に新項目Aで示した個別制限項目が新たに登録される。ステップS908で、要求に応じた制限項目を制御メニュー作成部112に通知する。制御メニュー作成部112は、図29に示されるサービス情報のうち、図31に示される個別制限項目でアクセスが許可されているものを選択し、制御メニューとする。その結果、制御端末141では図33に示すように、ビデオA151、ビデオB152、ビデオC1054の制御メニューが表示される。

【0160】一方、ユーザ（花子）が制御端末141より制御メニューを要求した場合、上記と同様の処理によって図31に示す新項目Bが新たに登録され、制御メニュー作成部112は、太郎の場合と同様に、図29に示されるサービス情報のうち、図31に示される個別制限項目でアクセスが許可されているものを選択し、制御メニューとする。その結果、制御端末141では図34に示すように、ビデオB152の制御メニューのみが表示される。

【0161】なお、個別制限項目格納部133に格納されている個別制限項目は、入力部134よりユーザが設定することができる。これは、制限項目作成部1031で作成されて登録された制限項目についても同様である。

【0162】なお、本実施形態では、宅外からのアクセスとして、インターネット160に接続されている制御端末141より制御メニューを要求したが、宅外ネットワークはインターネット以外でもよく、また、宅内のIEEE1394バス170またはその他のネットワークに接続されている制御端末より制御メニューを要求し、被制御装置を制御しても構わない。

【0163】また、本実施形態では、ユーザIDとして「太郎」を例にあげたが、これはユーザを識別するIDの例であり、ユーザに合わせて設定してもよい。また、ユーザに関する条件として、「太郎」や「花子」といった個人を対象としたユーザIDを用いて説明したが、ユーザの属性、例えばネットワーク管理者、家族、ゲストなどで分類した条件を用いても構わない。

【0164】また、本実施形態では、被制御端末が接続されるネットワークとしてIEEE1394バス170、制御端末が接続されるネットワークとしてインター

ネット160を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、ECHONETやBluetoothなどが挙げられる。

【0165】また、本実施形態では、2つのネットワークが通信装置1000に接続される例を示したが、これに限らず、通信装置1000に接続されるネットワークの数は1つまたは3以上であっても構わない。

10 【0166】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、2つの機器が連携して提供されるサービス、例えば、ビデオのダビングや通信路設定などであっても構わない。

【0167】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、サービス情報や、被制御端末が属するネットワークの情報や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用

20 しても構わない。  
【0168】また、本実施形態では、被制御端末として、ビデオA、ビデオB、およびビデオCを例に挙げたが、ビデオAが通信装置を通じてビデオBを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

【0169】また、本実施形態では、機器カテゴリーの分類項目としてビデオを使用した。AV機器や空調機器など他の分類を行っても構わない。

30 【0170】また、本実施形態では、制限項目を作成する際、個別制限項目をもとに制限情報の論理積をとることにより制限項目を作成したが、これに限らず、例えば制限情報の論理和や多数決を取って作成しても構わない。

【0171】また、本実施形態では、ネットワーク情報格納部123に格納されている要素情報に基づいて制御の制限を行ったが、それに代えて、制御メニュー作成部112から要素情報を要求された時点で、ネットワーク情報取得部122が要素情報を取得して制御メニュー作成部112に通知するようにしても構わない。要素情報を格納しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、要素情報を必要に応じて取得する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

40 【0172】また、本実施形態では、制御メニューを作成する際に新たな条件に合致する制限項目の作成を行ったが、これに限らず、それ以前のタイミングで作成しても構わない。例えば、新たな構成要素が検出された段階でこれを行ってもよい。この場合、制御メニューを作成する際に作成する場合と比較し、ユーザが制御メニューを要求してから、制御メニューを受け取るまでの時間が

納部 133 は、その結果を制限項目作成部 1831 に通知する。制限項目作成部 1831 は、通知された制限項目の数を数え、その結果、その数が 3 個より少ない場合、図 38 に示すように、第 2 の実施形態と同様の処理を行う。すなわち、制限項目作成部 1831 は、初期制限項目格納部 132 に対し、GUID を除いた条件を送信し、初期制限項目格納部 132 は、予め登録されている初期制限項目の中から、この条件に一致する制限項目を検索し、制限項目作成部 1831 に対して通知する。図 40 に、初期制限項目格納部 132 に格納されている初期制限項目の一例を示す。制限項目作成部 1831 は、通知された制限情報を条件と対応付けて、制限項目として個別制限項目格納部 133 に登録するとともに、制御メニュー作成部 112 に対して、要求された制限項目を通知する。

【0183】一方、制限項目作成部 1831 において、通知された制限項目の数を数えた結果、その数が 3 個以上だった場合には、図 41 に示すように、第 3 の実施形態と同様の処理を行う。すなわち、制限項目作成部 1831 は、個別制限項目格納部 133 より受け取った、他の機器に適用するために登録されている制限項目に基づいて制限情報を決定し、制限項目を作成する。具体的には、制限情報のアクセス許可を 1、アクセス不可を 0 とし、取得した制限情報で論理積をとって、制限情報を決定する。このように論理積を取ることで、設定されたすべての制限情報がアクセス許可でなければ、新たに接続された機器およびサービスもアクセス可能とはならず、不用意にアクセスを許可することがない。制限項目作成部 1831 は、決定した制限情報を条件と対応付けて、制限項目として個別制限項目格納部 133 に登録するとともに、制御メニュー作成部 112 に対して、要求された制限項目を通知する。

【0184】制御メニュー作成部 112 に対して、要求された制限項目を通知した以降の動作については、第 2 の実施形態および第 3 の実施形態と同様であるため、説明を省略する。

【0185】図 42 に示すフローチャートを参照して、制限項目作成部 1831 の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部 123 に図 37 に示す要素情報が格納されており、初期制限項目格納部 132 に図 40 に示す初期制限項目が格納されており、図 39 に示す個別制限項目において、GUID が「0x0123456789012345」である被制御端末 151 に関する制限項目（図中の新項目 A～F）を除く制限項目が登録されている状況を想定して説明する。ただし、図 42 において、図 25 または図 32 に示すフローと同一の処理ステップについては同一の参照符号を付し、説明を省略する。

【0186】制限項目作成部 1831 は、ステップ S901 からステップ S903 において、制御メニュー作成

部 112 から受け取った条件を個別制限項目格納部 133 に通知し、個別制限項目格納部 133 より条件に応じた制限情報を取得する。ここで取得する項目は以下の通りである。

【0187】GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=電源

制限情報=

GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=録画

制限情報=

GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=再生

制限情報=

GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=早送り

制限情報=

GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=巻き戻し

制限情報=

GUID=0x0123456789012345

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=停止

制限情報=

GUID=0x0123456789123456

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=電源

制限情報=アクセス許可

GUID=0x0123456789123456

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=録画

制限情報=アクセス不可

GUID=0x0123456789123456

ユーザ ID=太郎

制御端末のネットワーク情報=インターネット

サービス情報=再生

制限情報=アクセス許可

短くなるという利点がある。

【0173】 以上のように、第3の実施形態によれば、対応する個別制限項目が存在しない場合、すでに登録されている個別制限項目より、制限情報の論理和や論理積、多数決を取ることで、対応する個別制限項目を作成するので、初期制限項目を保持する必要が無く、必要とするメモリの容量を低減することができる。また、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【0174】 また、機器カテゴリーに応じてアクセス制限を設定しているため、例えばビデオなどのAV機器についてはセキュリティを甘くし、空調機器などについてはセキュリティを高めるというように、利便性と安全性を両立した制御が可能となる。

【0175】 (第4の実施形態) 以下、本発明の第4の実施形態に係る通信装置について、図面を参照しながら説明する。図35に、本実施形態に係る通信装置1800と、それに接続されるネットワークおよび制御端末、被制御端末とを示す。図35において、通信装置1800は、制御メニュー作成部110と、ディレクトリ管理機能部120と、制限項目管理部1830とを含む。制御メニュー構成部110は、制御メニュー作成要求受信部111と、制御メニュー作成部112と、制御メニュー送信部113とを含む。ディレクトリ管理機能部120は、ネットワーク構成要素検出部121と、ネットワーク情報取得部122と、ネットワーク情報格納部123とを含む。制限項目管理部1830は、制限項目作成部1831と、初期制限項目格納部132と、個別制限項目格納部133と、入力部134とを含む。通信装置1800は、インターネット160と、IEEE1394バス170に接続され、それらネットワークには、それぞれ制御端末141 (例えば、携帯電話) およびAV/Cコマンドを実装した被制御端末151~153 (例えば、ビデオA、ビデオB、チューナ) が接続される。なお、図35において、図17と同一の構成には同一の参照符号を付し、その説明を省略する。

【0176】 以下、通信装置1800の動作を、特に第2の実施形態に係る通信装置1000および第3の実施形態に係る通信装置1000との相違点を中心に説明する。ここでは、例として、機器151が新たに接続され、機器151、152、1054をユーザ (太郎) がインターネット160に接続された機器141から制御するために制御メニューを要求する場合について説明を行う。

【0177】 図36に、機器151がIEEE1394バス170に接続されたときの動作シーケンスを示す。図36に示すように、第2の実施形態と同様の動作により、ネットワーク情報格納部123に要素情報が更新され登録される。図37に、ネットワーク情報格納部12

3に格納される要素情報の一例を示す。

【0178】 制御メニュー構成部110は、第2の実施形態と同様に、制御端末141からの要求に応じて制御メニューを作成する。このとき、制限項目管理部1830に対して、制限項目を要求する。制限項目管理部1830では、制御メニュー作成部112から通知される条件に応じた制限項目を制御メニュー作成部112に対して返すのであるが、個別制限項目格納部133に条件に合致した制限項目が存在しなかった場合に、すでに個別制限項目格納部133に格納されている制限項目のうち、この条件に対応する制限項目を作成するのに必要な制限項目が一定数以上存在するときには、第3の実施形態と同様に、これら制限項目に基づいて条件に合致した制限項目を作成する。一方、条件に対応する制限項目を作成するのに必要な制限項目が一定数以上存在していないときには、第2の実施形態と同様に、初期制限項目格納部132に格納されている初期制限項目に基づいてこの条件に対応する制限項目を作成する。以下、その具体的な動作について説明する。

【0179】 図38に、インターネットに接続された携帯電話141を使用して、ユーザIDとして太郎で登録されているユーザが被制御端末151を制御するための制御メニューを取得する際の動作シーケンスを示す。制御端末141で制御メニューを要求してから制限項目作成部1831に制限項目要求が発行されるまでの動作については、第2の実施形態および第3の実施形態と同様であるので説明を省略する。

【0180】 制限項目作成部1831は、受け取った条件を個別制限項目格納部133に送り、制限項目の発行を要求する。個別制限項目格納部133は、受け取った条件に合致する制限情報を検索して制限項目作成部1831に通知する。図39に、個別制限項目格納部133に格納されている制限項目の一例を示す。

【0181】 なお、図39に示すのは、新たに接続された機器151に関する個別制限項目 (図39に新項目A~Fで示す) が後述する処理によって新たに登録された後の内容を示している。ここでは、これら新項目A~Fが、まだ登録されていない状態を仮定して説明を行っている。なお、図39では、制限項目の条件として、サービス情報による条件が含まれている場合を示している。

【0182】 ここで、被制御端末151は、新たにIEEE1394バス170に追加された機器であるため、個別制限項目格納部133には被制御端末151のGUIDは登録されていない。制限項目作成部1831は、GUIDの一致する制限項目が個別制限項目格納部133に登録されていなかった場合、他の機器に適用するために登録されている制限項目の中から、この条件と「ユーザID」、「機器カテゴリー」、および「制御端末のネットワーク情報」が一致する制限項目の検索を個別制限項目格納部133に対して要求する。個別制限項目格

GUID=0x0123456789123456  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=早送り  
 制限情報=アクセス許可  
 GUID=0x0123456789123456  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=巻き戻し  
 制限情報=アクセス許可  
 GUID=0x0123456789123456  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=停止  
 制限情報=アクセス許可  
 GUID=0x0123456789234567  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=電源  
 制限情報=アクセス許可  
 GUID=0x0123456789234567  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=選局  
 制限情報=アクセス許可  
 【0188】ステップS904で、制限情報が存在しない条件があるか確認する。存在すればステップS1609に進み、存在しなければステップS908に進む。ここでは、GUID=0x0123456789012345の条件がこれにあたる。ステップS1609で、個別制限項目格納部133に対して、制限情報が存在しない条件について、GUID以外の条件に合致する制限項目を通知するように要求する。ステップS1610で、前のステップS1609で要求した制限項目を受け取る。ここで受け取る項目は以下の通りである。  
 【0189】ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=電源  
 制限情報=アクセス許可  
 個数=2  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=録画  
 制限情報=アクセス不可  
 個数=1  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=再生  
 制限情報=アクセス許可  
 個数=1

ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=早送り  
 制限情報=アクセス許可  
 個数=1  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=巻き戻し  
 制限情報=アクセス許可  
 個数=1  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=停止  
 制限情報=アクセス許可  
 個数=1  
 【0190】ステップS2612で、受け取った制限項目の数が閾値で定めた3以上であるか否かを判定し、3より少ない場合はステップS905およびステップS906を実行し、3以上の場合はステップS1611に進む。この例では、個数は1または2であるので、ステップS905に進む。  
 【0191】ステップS905で、制限情報が存在しない条件について、初期制限項目格納部132に対して、この条件に対応する制限項目を通知するように要求する。ステップS906で、前のステップS905の要求に対する条件に一致する制限項目を受け取る。ここで受け取る項目は以下の通りである。  
 【0192】ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=電源  
 制限情報=アクセス許可  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=録画  
 制限情報=アクセス不可  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=再生  
 制限情報=アクセス許可  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=早送り  
 制限情報=アクセス許可  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=巻き戻し  
 制限情報=アクセス許可  
 ユーザID=太郎  
 制御端末のネットワーク情報=インターネット  
 サービス情報=停止

制限情報＝アクセス許可

【0193】一方、ステップS1611では、前のステップS1610で受け取った制限情報に対して、論理積を取り、それをこのGUIDである機器のサービスに対する制限情報とする。

【0194】ステップS907で、ステップS906で受け取りまたはステップS1610で作成した制限項目を、個別制限項目格納部133に登録する。この結果、図39に新項目A～Fで示した個別制限項目が新たに登録される。ステップS908で、条件と制限情報を対応付けて、制御メニュー作成部112に通知する。制御メニュー作成部112は、図37に示されるサービス情報のうち、図39に示される個別制限項目でアクセスが許可されているものを選択し、制御メニューとする。その結果、制御端末141では図43に示すように、ビデオA151、ビデオB152、チューナ153の制御メニューが表示される。

【0195】なお、本実施形態では、閾値は3を使用した。これに限らず、他の値、例えば1や2、または4以上の値を使用しても構わない。

【0196】なお、個別制限項目格納部133に格納されている個別制限項目は、入力部134よりユーザが設定することができる。これは、制限項目作成部1831で作成されて登録された制限項目についても同様である。また、初期制限項目格納部132に格納されている初期制限項目についても、入力部134よりユーザが設定することができる。

【0197】なお、本実施形態では、宅外からのアクセスとして、インターネット160に接続されている制御端末141より制御メニューを要求したが、宅外ネットワークはインターネット以外でもよく、また、宅内のIEEE1394バス170またはその他のネットワークに接続されている制御端末より制御メニューを要求し、被制御装置を制御しても構わない。

【0198】また、本実施形態では、ユーザIDとして「太郎」を例にあげたが、これはユーザを識別するIDの例であり、ユーザに合わせて設定してもよい。また、ユーザに関する条件として、「太郎」という個人を対象としたユーザIDを用いて説明したが、ユーザの属性、例えばネットワーク管理者、家族、ゲストなどで分類した条件を用いても構わない。

【0199】また、本実施形態では、被制御端末が接続されるネットワークとしてIEEE1394バス170、制御端末が接続されるネットワークとしてインターネット160を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、ECHONETやBluetoothなどが挙げられる。

【0200】また、本実施形態では、2つのネットワー

クが通信装置1800に接続される例を示したが、これに限らず、通信装置1800に接続されるネットワークの数は1つまたは3以上であっても構わない。

【0201】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、2つの機器が連携して提供されるサービス、例えば、ビデオのダビングや通信路設定などであっても構わない。

【0202】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、機器のカテゴリーや、被制御端末が属するネットワークの情報や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【0203】また、本実施形態では、被制御端末として、ビデオA、ビデオBおよびチューナを例に挙げたが、チューナが通信装置を通じてビデオAを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

【0204】また、本実施形態では、機器カテゴリーの分類項目としてビデオやチューナを使用した。AV機器や空調機器など他の分類を行っても構わない。

【0205】また、本実施形態では、制限項目を作成する際、個別制限項目をもとに制限情報の論理積を取ることにより制限項目を作成したが、これに限らず、例えば制限情報の論理和や多数決を取って作成しても構わない。

【0206】また、本実施形態では、ネットワーク情報格納部123に格納されている要素情報に基づいて制御の制限を行ったが、それに代えて、制御メニュー作成部112から要素情報を要求された時点で、ネットワーク情報取得部122が要素情報を取得して制御メニュー作成部112に通知するようにしても構わない。要素情報を格納しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、要素情報を必要に応じて取得する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【0207】また、本実施形態では、制御メニューを作成する際に新たな条件に合致する制限項目の作成を行ったが、これに限らず、それ以前のタイミングで作成しても構わない。例えば、新たな構成要素が検出された段階でこれを行ってもよい。この場合、制御メニューを作成する際に作成する場合と比較し、ユーザが制御メニューを要求してから、制御メニューを受け取るまでの時間が短くなるという利点がある。

【0208】以上のように、第4の実施形態によれば、対応する個別制限項目が存在しない場合において、すでに登録されている個別制限項目が少ない場合は、初期制限項目を用いてアクセス制限を行い、一方、登録されている個別制限項目が多い場合は、すでに登録されている

個別制限項目より、論理和や論理積や多数決を取ること  
で対応する個別制限項目を作成するので、参照する個別  
制限項目が少ないために発生するアクセス制限の偏りを  
防ぎながら、実際に設定されているアクセス制限の傾向  
を反映することが可能となる。さらに、ユーザがアクセ  
ス制限をその都度設定する必要がなく、よって、新たに  
使用するサービスに対して、アクセス設定をサービス毎  
に行うことなく使用することができる。

【0209】また、サービスの種類に応じてアクセス制  
限の設定を行っているため、例えば再生は可能とする  
が、録画は禁止するというように、利便性と安全性を両  
立した制御が可能となる。

【0210】（第5の実施形態）以下、本発明の第5の  
実施形態に係る通信装置について、図面を参照しながら  
説明する。図44に、本実施形態に係る通信装置270  
0と、それに接続されるネットワークおよび制御端末、  
被制御端末とを示す。図44において、通信装置270  
0は、制御コマンド中継部2710と、ディレトリ管  
理機能部2720と、制限項目管理部130とを備え  
る。制御コマンド中継部2710は、制御コマンド送受  
信部2713と、制御コマンド判定部2712とを含  
む。ディレトリ管理機能部2720は、ネットワーク  
構成要素検出部121と、ネットワーク情報取得部12  
2と、ネットワーク情報格納部123と、インターネッ  
トプロトコルをIEEE1394プロトコルに変換する  
IEEE1394プロトコル変換部2724と、インター  
ネットプロトコルをECHONETプロトコルに変換  
するECHONETプロトコル変換部2725とを含  
む。制限項目管理部130は、制限項目作成部131  
と、初期制限項目格納部132と、個別制限項目格納部  
133と、入力部134とを含む。

【0211】通信装置2700は、インターネット16  
0、IPネットワーク2780、IEEE1394バス  
170、およびECHONET2790の各ネットワ  
ークに接続される。インターネット160には、制御端末  
141（例えば携帯電話）が接続され、IPネットワ  
ーク2780には、被制御端末2755（例えばPC）が  
接続され、IEEE1394バス170には、AV/C  
コマンドを実装した機器である被制御端末2756（例  
えばビデオ）が接続され、ECHONET2790に  
は、被制御端末2757（例えばエアコン）が接続され  
ている。ここで、インターネット160を宅外ネットワ  
ーク、その他のネットワーク2780、170、279  
0を宅内のネットワークとする。

【0212】なお、図44において、図17と同一の構  
成には同一の参照符号を付し、説明を省略する。以下、  
通信装置2700の動作を説明する。この動作を示す例  
として、宅外のインターネット160に接続された機器  
141を利用して、宅内の機器2757を初めて使用する  
場合について説明を行う。

【0213】図45に、ネットワーク情報格納部123  
が、サービスの制御メニューを作成するために機器のサ  
ービス情報を取得する際のシーケンスを示す。

【0214】ネットワーク情報格納部123は、ネット  
ワーク情報取得部122に対して、宅内ネットワークに  
接続されている機器のサービス情報を収集するように要  
求する。ネットワーク情報取得部122は、サービス情  
報取得要求を受け取ると、各ネットワークに接続されて  
いる被制御端末（エアコン）2757、被制御端末（ビ  
デオ）2756、被制御端末（PC）2755に対し、  
サービス情報を通知するように要求する。このとき、ビ  
デオ2756およびエアコン2757は、接続されてい  
るネットワークが異なるため、それぞれIEEE139  
4プロトコル変換部2724およびECHONETプロ  
トコル変換部2725を通してプロトコル変換を行うこ  
とで、要求を発行する。

【0215】エアコン2757、ビデオ2756、およ  
びPC2755は、サービス情報取得要求に対し、その  
機器がネットワークに提供できるサービスの制御コマン  
ドを、ネットワーク情報取得部122に送信する。この  
とき、あわせて、予め登録されてある機器の名前と機器  
カテゴリーとサービス名も通知する。機器カテゴリー  
は、PCやAV機器や空調機器などといった機器の種類  
を示す。機器の名前およびサービス名は、ユーザがその  
サービスを識別するために使用するものであり、  
機器の名前としては、例えばPCやビデオなどであり、  
サービス名としては、制御コマンドの動作を示す名前、  
例えば録画や再生などが望ましい。

【0216】ネットワーク情報取得部122は、各機器  
から収集したサービス情報等の情報をネットワーク情報  
格納部123に登録する。図46に、ネットワーク情報  
格納部123に格納される情報の一例を示す。ネットワ  
ーク情報格納部123は、その登録された情報に基づい  
て制御メニューを作成する。

【0217】図47に、宅外のインターネット160に  
接続された携帯電話141を使用して、通信装置270  
0より制御メニューを取得し、その制御メニューにある  
制御コマンドを発行して宅内ネットワーク2790のエ  
アコン2757を制御するときの動作シーケンスを示  
す。ユーザは、携帯電話141を操作して、通信装置2  
700が保持している制御メニューを送信するよう通信  
装置2700に対して要求する。メニュー要求を受けた  
通信装置2700の制御コマンド送受信部2713は、  
ネットワーク情報格納部123が保持している制御メ  
ニューを要求し、これを受けて、ネットワーク情報格納部  
123は、制御コマンド送受信部2713に対し制御メ  
ニューを送信する。

【0218】制御コマンド送受信部2713は、制御端  
末141に対し、制御メニューを送信する。制御メ  
ニューは、制御端末141で実行可能なアプリケーションの

形式でもよいが、好ましくは、HTMLで記述されたソースであることが望ましい。この場合、制御端末141は、HTMLブラウザを装備していれば、機器の制御を行うことが可能となる。また、制御メニューで表示される項目と制御コマンドとがCGIなどで関連付けられていることが望ましい。

【0219】次に、ユーザは、制御メニューに基づいて制御端末141を操作し、希望する制御コマンドを発行する。コマンド発行時には、制御対象の機器識別子の情報もあわせて送られる。ここで、機器識別子は、宅内ネットワークに接続されている機器を、通信装置2700が一意に識別するためのものであり、ネットワーク情報格納部123が、各ネットワークに固有のアドレス体系から作成するものである。

【0220】制御端末141から発行された制御コマンドは、制御コマンド送受信部2713で受信され、制御コマンド送受信部2713は、受信したコマンドおよび機器識別子を、制御コマンド判定部2712に転送する。このとき、あわせて、制御端末141が属するネットワーク情報も通知する。制御コマンド判定部2712は、ネットワーク情報格納部123に対し、機器識別子に対応する機器カテゴリーを通知するように要求する。ネットワーク情報格納部123は、この要求を受けて、機器カテゴリーを通知する。

【0221】次に、制御コマンド判定部2712は、制限項目作成部131に対し、制御端末141から受信した制御コマンドに対する制限情報を通知するように要求する。このとき、制限情報を検索するための条件として、機器識別子と、制御端末のネットワーク情報と、機器カテゴリーと、制御コマンドとをあわせて送信する。ここで、制限情報は、制御コマンドを使用することができるか否を示す。

【0222】制限項目作成部131は、受け取った機器識別子および制御端末のネットワーク情報をあわせて、個別制限項目格納部133に制限項目要求を発行する。図48に、個別制限項目格納部133に格納されている制限項目の一例を示す。ただし、図48に示すのは、新たに接続された機器2575に関する個別制限項目（図48に新項目Aで示す）が後述する処理によって新たに登録された後の内容を示している。ここでは、この新項目Aが、まだ登録されていない状態を仮定して説明を行っている。個別制限項目格納部133は、受け取った機器識別子と制御端末のネットワーク情報に合致する制限項目を検索し、制限項目作成部131に通知する。制限項目作成部131が、個別制限項目格納部133に条件に合致する制限項目がないと判断した場合、制限項目作成部131は、初期制限項目格納部132に対し、制御端末のネットワーク情報と、機器カテゴリーとを送信する。初期制限項目格納部132は、初期制限項目の中から、この条件に一致する制限項目を検索し、制限項目作

成部131に対して通知する。図49に、初期制限項目格納部132に格納される初期制限項目の一例を示す。ここで、エアコン2757は、宅外ネットワークから初めて制御されるため、エアコン2757の機器識別子は個別制限項目格納部133には登録されていない。よって、制限項目作成部131は、初期制限項目格納部132から条件に合致する制限項目を取得することになる。制限項目作成部131は、通知された初期制限項目と、機器識別子と、制御端末のネットワーク情報とを対応づけて、個別制限項目格納部133に登録する。

【0223】制限項目作成部131は、制御コマンド判定部2712に対して、制限項目と、機器識別子と、制御端末のネットワーク情報とを通知する。制御コマンド判定部2712は、通知された制限項目に基づいて、受信した制御コマンドを発行してもよいか否か判定する。制限項目においてアクセス許可になっている場合は、制御コマンド判定部2712は、受信した制御コマンドをECHONETプロトコル変換部2725に発行する。ECHONETプロトコル変換部2725は、ECHONETの仕様に従って制御コマンドの変更などを行い、エアコン2757に対して制御コマンドを発行する。

【0224】図50に示すフローチャートを参照して、制限項目作成部131の動作を説明する。以下では、説明を分かり易くするために、具体例として、ネットワーク情報格納部123に図46に示す情報が格納されており、初期制限項目格納部132に図49に示す初期制限項目が格納されており、図48に示す個別制限項目において、宅外ネットワークであるインターネット160に接続されている制御端末141に係る制限項目（図中の新項目A）が未登録である状況を想定して説明する。ただし、図50において、図25に示すフローと同一の処理ステップについては同一の参照符号を付す。

【0225】制限項目作成部131は、ステップS901で、制御コマンド判定部2712より、制限項目を作成する際の条件として、機器識別子と、制御端末のネットワーク情報と、機器カテゴリーとを受け取る。ここで受け取る項目は以下の通りである。

【0226】機器識別子=0x0003

制御端末のネットワーク情報=宅外

機器カテゴリー=空調機器

【0227】ステップS902で、機器識別子と制御端末のネットワーク情報とをもとに、個別制限項目格納部133に対し個別制限項目を送るよう要求する。ステップS903で、ステップS902の要求に対する条件に一致する制限項目を受け取る。ただし、ここでの説明の例では、条件に対応した制限項目がなかったことが通知される。ステップS904で、制限情報がない条件が存在するか否かを確認する。制限情報がない条件が存在すれば、以下のステップS905に進み、存在しなければ、ステップS908に進む。ここでの説明の例では、

ステップ S 905 に進む。

【0228】ステップ S 905 で、制限情報が存在しない条件について、初期制限項目格納部 132 に対して、この条件に対応する制限項目を通知するように要求する。ステップ S 906 で、ステップ S 905 の要求に対する条件に一致する制限情報を受け取る。ここで受け取る項目は以下の通りである。

【0229】制御端末のネットワーク情報＝宅外  
機器カテゴリ＝空調機器  
制限情報＝アクセス許可

【0230】ステップ S 907 で、ステップ S 906 で受け取った制限項目を個別制限項目格納部 133 に登録する。この結果、図 48 に新項目 A で示した個別制限項目が新たに登録される。ステップ S 908 で、条件と制限情報とを対応づけて、制御コマンド判定部 2712 に通知する。この結果、宅外ネットワークからエアコン 2757 を制御することは、制限情報＝アクセス許可であるため、制御コマンド判定部 2712 は、制御端末 141 に対して、実行許可の通知を行う。なお、このとき、通知された制限情報がアクセス不可であった場合には、制御コマンド判定部 2712 は、制御コマンド送受信部 2713 を通じて制御端末 141 に対し制御不可の通知を行い、制御端末 141 は、その通知を受けて、例えば「この制御コマンドに対する権限を有しておりません」等の画面表示を行う。

【0231】なお、個別制限項目格納部 133 に格納されている個別制限項目は、入力部 134 よりユーザが設定することができる。これは、制限項目作成部 131 で作成されて登録された制限項目についても同様である。また、初期制限項目格納部 132 に格納されている初期制限項目についても、入力部 134 よりユーザが設定することができる。

【0232】なお、本実施形態では、宅外からのアクセスとして、インターネット 160 に接続されている制御端末 141 より制御コマンドの発行を行ったが、宅外ネットワークはインターネット以外でもよく、また、宅内の IP ネットワーク 2780 や IEEE 1394 バス 170 や ECHONET 2790 またはその他のネットワークに接続されている制御端末より制御コマンドの発行を行って、被制御端末を制御しても構わない。例えば、宅内からのアクセスとして、PC 2755 より制御コマンドを発行して被制御装置を制御しても構わない。

【0233】また、本実施形態では、宅内のネットワークとして IEEE 1394 バス 170、IP ネットワーク 2780、ECHONET 2790 を取り上げ、宅外のネットワークとしてインターネット 160 を取り上げたが、いずれもこれに限らず、他のネットワークでも構わない。さらに、有線であっても、無線であっても構わない。他のネットワークの例として、Bluetooth などが挙げられる。

【0234】また、本実施形態では、4つのネットワークが通信装置 2700 に接続される例を示したが、これに限らず、通信装置 2700 に接続されるネットワークの数は1から3または5以上であっても構わない。

【0235】また、本実施形態で取り上げたサービスは機器毎に提供されるサービスであったが、これに限らず、2つの機器が連携して提供されるサービス、例えば、ビデオのダビングや通信路設定などであっても構わない。

10 【0236】また、制限項目の条件として、本実施形態で使用したパラメータ以外にも、任意のパラメータを使用しても構わない。例えば、機器のカテゴリや、サービス情報や、ユーザ ID や、使用する時間や、表示能力・音声再生能力といった機器の処理能力等を使用しても構わない。

【0237】また、本実施形態では、被制御端末として、PC、ビデオ、およびエアコンを例に挙げたが、PC が通信装置を通じてビデオを制御するなど、これらの機器が制御端末となって他の被制御機器を制御しても構わない。

20 【0238】また、本実施形態では、機器カテゴリの分類項目として AV 機器や空調機器などを使用したか、ビデオやチューナなど他の分類を行っても構わない。

【0239】また、本実施形態では、ネットワーク情報格納部 123 に格納されている要素情報に基づいて予めメニューを作成しておくとしたが、それに代えて、制御コマンド送受信部 2713 からメニューを要求された時点で、ネットワーク情報取得部 122 が要素情報を取得してメニューを作成するようにしても構わない。予めメニューを作成しておく場合には、ユーザの操作に対するレスポンスが向上するという利点があり、一方、メニューを必要に応じて作成する場合には、要素情報を格納しておくための記憶容量が不要になるという利点がある。

【0240】また、本実施形態では、制御端末 141 から制御コマンドを発行した際に新たなサービスに係る制限項目の作成を行ったが、新たなサービスを検出した段階でこれを行っても構わない。この場合、前者と比較し、ユーザが制御コマンドを発行してから、制御コマンド中継部 2710 がこの制御コマンドの有効性を判断して被制御端末に向けて発行するまでの時間が短くなるため好ましい。

【0241】以上のように、第5の実施形態によれば、対応する個別制限項目が存在しない場合、初期制限項目を用いてアクセス制限を行うため、ユーザがアクセス制限をその都度設定する必要がなく、よって、新たに使用するサービスに対して、アクセス設定をサービス毎に行うことなく使用することができる。

【0242】また、通信装置がユーザに対して送信する制御メニューにアクセス制限の内容を反映させる前述の第2の実施形態等と比較し、制御端末が発行した制御コ



マンドに対してアクセス制限を行うことができる。

【0243】また、制御端末および被制御端末のネットワークによってアクセス制限を設定しているため、例えば宅外ネットワークとしてインターネットのように不特定多数が利用するネットワークに対してはアクセス不可とし、IEEE1394バスのような宅内のネットワークであればアクセス許可するというように、利便性と安全性を両立した制御が可能となる。

【0244】次に、本件発明の実施形態から把握できる請求項以外の技術思想を、その効果とともに記載する。

【0245】第1の発明は、単一または複数のネットワークに接続され、このネットワークに接続される複数の機器のうちのある機器による他の機器に対する制御を条件に応じて制限する通信装置であって、ネットワークおよびネットワークに接続される機器に関する情報を要素情報として取得するディレクトリ管理手段と、要素情報と、他の機器を制御する機器である制御端末に関する情報と、この制御端末を使用して制御を行おうとするユーザの識別子との少なくともいずれかを含む情報を制御条件として、この制御条件に合致する場合の制御の可否を規定する制限情報とともに個別制限項目として管理する制限項目管理手段と、要素情報および個別制限項目に基づいて、機器間の制御を制限する制御制限手段とを備え、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、この制御条件に応じてこの制御条件に係る個別制限項目を動的に新たに作成することを特徴とする。

【0246】上記のように、第1の発明によれば、ネットワーク上に新たな機器が接続されたときなど、ネットワーク上の機器間で制御を行う際に、その制御の可否を示す情報が登録されていない場合であっても、この制御の可否を示す制限項目を動的に作成するため、ユーザがその都度設定を行う必要がなく、ネットワークに対して十分な知識がないユーザがネットワーク機器を接続した場合でも、ネットワークのセキュリティを確保したまま、ネットワークを通じて制御することが可能となる。またこのとき、ネットワークに接続される機器に関する情報や、制御端末に関する情報、例えば、制御端末が所属するネットワークに関する情報や表示能力・再生能力等の制御端末の性能に関する情報や、制御を行おうとするユーザの識別子の情報やその他種々の条件またはその組合せに応じて、動的に好ましい設定を行うことができる。

【0247】第2の発明は、第1の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納手段を含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴

とする。

【0248】上記のように、第2の発明によれば、個別制限項目に存在しない制御条件に対して制限を行うために、予め設定された初期制限項目から制御条件に合致した好ましい制限項目を作成するので、例えば新たな機器がネットワークに接続された際でも、その機器に対して予め設定された初期制限項目に基づいて好ましい設定を自動的に設定することができる。

【0249】第3の発明は、第1の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、この選出された個別制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【0250】上記のように、第3の発明によれば、制御条件に合致した個別制限項目が登録されていない場合であっても、すでに登録されている個別制限項目の中から、この制御条件が一部の条件を除いて一致するものをもとに、この制御条件に対する制御の可否を自動的に設定することができる。なお、一部の条件としては、例えば、機器識別子や、制御端末を操作するユーザの識別子などであり、これにより、例えば、ネットワークに新たな機器が接続され、この機器の識別子に対する制限項目がまだ登録されていない場合であっても、すでに登録されている個別制限項目の中からこの機器の識別子を除いて条件が一致するものを参照して類推することにより、予め特別な設定を必要とすることなく、好ましい設定を自動的に行うことができる。

【0251】第4の発明は、第3の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、選出した個別制限項目に含まれる制限情報の全てにおいて制御許可が規定されている場合には、この制御条件に係る個別制限項目として、制御許可を規定する制限情報を含む個別制限項目を新たに作成し、一方、選出した個別制限項目に含まれる制限情報のいずれかにおいて制御不許可が規定されている場合には、この制御条件に係る個別制限項目として、制御不許可を規定する制限情報を含む個別制限項目を新たに作成することを特徴とする。

【0252】上記のように、第4の発明によれば、制御を制限しようとする制御条件に対して、選出した個別制限項目において全て制御許可である場合のみ、制御許可として制限情報を設定するため、自動的に制限項目を設定することによって、本来制御が許可されるべきでない条件に対して、勝手に制御許可として登録してしまう危

険を回避し、より安全に制限項目の自動設定が行える。

【0253】第5の技術思想は、第1の発明において、制限項目管理手段は、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納手段を含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在する場合には、この制御条件に関連する個別制限項目に含まれる制限情報に基づいて、この制御条件に係る個別制限項目を新たに作成し、一方、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在しない場合には、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【0254】上記のように、第5の発明によれば、制限項目がまだ登録されていない制御条件に対して、この制御条件に対する制限情報を類推するための個別制限項目が、一定数以上存在する場合にはそれら個別制限項目から類推して制限情報を設定し、一方、一定数以上存在しない場合には、初期制限項目に基づいて設定する。よって、制御条件に対して制限情報を類推するための材料となる個別制限項目が少ない場合に不十分な判断材料に基づいて望ましくない設定がなされてしまう危険が回避できる。

【0255】第6の発明は、第1の発明において、制御制限手段は、制限項目管理手段によって管理される個別制限項目に基づいて、制御端末が制御可能であるサービスについてのみからなる制御メニューをこの制御端末に送信することにより、制御端末による制御を制限することを特徴とする。

【0256】上記のように、第6の発明によれば、制御端末に通知する制御メニュー自体の内容に制限内容を反映させることにより、機器の制御を容易に制限することができる。また、制御を行おうとするユーザは、事前に制御可能な内容を知ることができるため、制御コマンドを実行するまで制御の可否が分からないという問題もなく機器の制御を行うことができる。

【0257】第7の発明は、第1の発明において、制御制限手段は、制限項目管理手段によって管理される個別制限項目に基づいて、制御端末が発行した制御コマンドのうち、この制御端末が制御可能であるサービスに係る制御コマンドのみを制御対象の機器に送信することにより、制御端末による制御を制限することを特徴とする。

【0258】上記のように、第7の発明によれば、ユーザが制御端末からコマンドが発生された時点で制御の可否を判断するため、例えば制限項目が変更された直後であっても、その変更内容が即座に制御の制限に反映され

ることになり、より確実な制限が容易に可能となる。

【0259】第8の発明は、第1の発明において、ディレクトリ管理手段は、ネットワークに新たな機器が接続されたことを検出する構成要素検出手段を含む。

【0260】上記のように、第8の発明によれば、ネットワークに新たな機器が接続されたときに、これを検出することができるため、ディレクトリ管理手段において最新の要素情報を自動的に取得することができる。

【0261】第9の発明は、第1の発明において、制御条件は、制御端末の属するネットワークが宅内のネットワークであるか宅外のネットワークであるかに関する条件を含む。

【0262】上記のように、第9の発明によれば、宅内からのアクセスか宅外からのアクセスかに応じて制御を制限することができるため、例えば、宅内からのアクセスは許可して、宅外からのアクセスは不可にするなど、安全性の高い設定を動的に設定することができる。

【0263】第10の発明は、単一または複数のネットワークに接続される複数の機器のうちのある機器による他の機器に対する制御を条件に応じて制限する通信制限方法であって、ネットワークおよびネットワークに接続される機器に関する情報を要素情報として取得するディレクトリ管理ステップと、要素情報と、他の機器を制御する機器である制御端末に関する情報と、この制御端末を使用して制御を行おうとするユーザの識別子との少なくともいずれかを含む情報を制御条件として、この制御条件に合致する場合の制御の可否を規定する制限情報とともに個別制限項目として管理する制限項目管理ステップと、要素情報および個別制限項目に基づいて、機器間の制御を制限する制御制限ステップとを備え、制限項目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、この制御条件に応じてこの制御条件に係る個別制限項目を動的に新たに作成することを特徴とする。

【0264】上記のように、第10の発明によれば、ネットワーク上に新たな機器が接続されたときなど、ネットワーク上の機器間で制御を行う際に、その制御の可否を示す情報が登録されていない場合であっても、この制御の可否を示す制限項目を動的に作成するため、ユーザがその都度設定を行う必要がなく、ネットワークに対して十分な知識がないユーザがネットワーク機器を接続した場合でも、ネットワークのセキュリティを確保したまま、ネットワークを通じて制御することが可能となる。またこのとき、ネットワークに接続される機器に関する情報や、制御端末に関する情報、例えば、制御端末が所属するネットワークに関する情報や表示能力・再生能力等の制御端末の性能に関する情報や、制御を行おうとするユーザの識別子の情報やその他種々の条件またはその組合せに応じて、動的に好ましい設定を行うことができる。

【0265】第11の発明は、第10の発明において、制限项目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納ステップを含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【0266】上記のように、第11の発明によれば、個別制限項目に存在しない制御条件に対して制限を行うために、予め設定された初期制限項目から制御条件に合致した好ましい制限項目を作成するので、例えば新たな機器がネットワークに接続された際でも、その機器に対して予め設定された初期制限項目に基づいて好ましい設定を自動的に設定することができる。

【0267】第12の発明は、第10の発明において、制限项目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、この選出された個別制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

【0268】上記のように、第12の発明によれば、制御条件に合致した個別制限項目が登録されていない場合であっても、すでに登録されている個別制限項目の中から、この制御条件が一部の条件を除いて一致するものをもとに、この制御条件に対する制御の可否を自動的に設定することができる。なお、一部の条件としては、例えば、機器識別子や、制御端末を操作するユーザの識別子などであり、これにより、例えば、ネットワークに新たな機器が接続され、この機器の識別子に対する制限項目がまだ登録されていない場合であっても、すでに登録されている個別制限項目の中からこの機器の識別子を除いて条件が一致するものを参照して類推することにより、予め特別な設定を必要とすることなく、好ましい設定を自動的に行うことができる。

【0269】第13の発明は、第12の発明において、制限项目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中から、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目を選出し、選出した個別制限項目に含まれる制限情報の全てにおいて制御許可が規定されている場合には、この制御条件に係る個別制限項目として、制御許可を規定する制限情報を含む個別制限項目を新たに作成し、一方、選出した個別制限項目に含まれる制限情報のいずれかにおいて制御不許可が規定されている場合には、この制御条件に係る個別制限項目として、制御不許可を規定する制限情報を含む個別制限項目を新たに作成

することを特徴とする。

【0270】上記のように、第13の発明によれば、制御を制限しようとする制御条件に対して、選出した個別制限項目において全て制御許可である場合のみ、制御許可として制限情報を設定するため、自動的に制限項目を設定することによって、本来制御が許可されるべきでない条件に対して、勝手に制御許可として登録してしまう危険を回避し、より安全に制限項目の自動設定が行える。

10 【0271】第14の発明は、第10の発明において、制限项目管理ステップは、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない時に適用される初期制限項目を格納する初期制限項目格納ステップを含み、制御端末が制御を行う際の制御条件に合致する個別制限項目が存在しない場合に、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在する場合には、この制御条件に関連する個別制限項目に含まれる制限情報に基づいて、この制御条件に係る個別制限項目を新たに作成し、一方、現時点において管理している個別制限項目の中に、この制御条件に対して一部の条件を除いて条件が一致する個別制限項目が所定数以上存在しない場合には、初期制限項目に基づいて、この制御条件に係る個別制限項目を新たに作成することを特徴とする。

30 【0272】上記のように、第14の発明によれば、制限項目がまだ登録されていない制御条件に対して、この制御条件に対する制限情報を類推するための個別制限項目が、一定数以上存在する場合にはそれら個別制限項目から類推して制限情報を設定し、一方、一定数以上存在しない場合には、初期制限項目に基づいて設定する。よって、制御条件に対して制限情報を類推するための材料となる個別制限項目が少ない場合に不十分な判断材料に基づいて望ましくない設定がなされてしまう危険が回避できる。

40 【0273】第15の発明は、第10の発明において、制御制限ステップは、制限项目管理ステップによって管理される個別制限項目に基づいて、制御端末が制御可能であるサービスについてのみからなる制御メニューをこの制御端末に送信することにより、制御端末による制御を制限することを特徴とする。

【0274】上記のように、第15の発明によれば、制御端末に通知する制御メニュー自体の内容に制限内容を反映させることにより、機器の制御を容易に制限することができる。また、制御を行おうとするユーザは、事前に制御可能な内容を知ることができるため、制御コマンドを実行するまで制御の可否が分からないという問題もなく機器の制御を行うことができる。

50 【0275】第16の発明は、第10の発明において、制御制限ステップは、制限项目管理ステップによって管

理される個別制限項目に基づいて、制御端末が発行した制御コマンドのうち、この制御端末が制御可能であるサービスに係る制御コマンドのみを制御対象の機器に送信することにより、制御端末による制御を制限することを特徴とする。

【0276】上記のように、第16の発明によれば、ユーザが制御端末からコマンドが発生された時点で制御の可否を判断するため、例えば制限項目が変更された直後であっても、その変更内容が即座に制御の制限に反映されることになり、より確実な制限が容易に可能となる。

【0277】第17の発明は、第10の発明において、ディレクトリ管理ステップは、ネットワークに新たな機器が接続されたことを検出する構成要素検出ステップを含む。

【0278】上記のように、第17の発明によれば、ネットワークに新たな機器が接続されたときに、これを検出することができるため、ディレクトリ管理手段において最新の要素情報を自動的に取得することができる。

【0279】第18の発明は、第10の発明において、制御条件は、制御端末の属するネットワークが宅内のネットワークであるか宅外のネットワークであるかに関する条件を含む。

【0280】上記のように、第18の発明によれば、宅内からのアクセスか宅外からのアクセスかに応じて制御を制限することができるため、例えば、宅内からのアクセスは許可して、宅外からのアクセスは不可にするなど、安全性の高い設定を動的に設定することができる。

#### 【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るファイアウォール装置の基本的構成を示す図である。

【図2】本発明の第1の実施形態に係るファイアウォール装置の内部ハードウェア基本構成を示すブロック図である。

【図3】本発明の第1の実施形態に係るファイアウォール装置のソフトウェア基本構成を示すブロック図である。

【図4】本発明の第1の実施形態に係るファイアウォール装置で行われる通信路設定処理の動作を示すフローチャートである。

【図5】図4のステップS104のサブルーチンを示すフローチャートである。

【図6】本発明の第1の実施形態に係るファイアウォール装置の認証サービスに対して、通信路が外部から設定される動作を示すフローチャートである。

【図7】本発明の第1の実施形態に係るファイアウォール装置が行うサービス有効期限管理の動作を示すフローチャートである。

【図8】本発明の第1の実施形態に係るファイアウォール装置のディレクトリ管理機能部に格納されているサービス情報の一例を示す図である。

【図9】本発明の第1の実施形態に係るファイアウォール装置のディレクトリ管理機能部に予め設定されているサービス基本公開ポリシーの一例を示す図である。

【図10】本発明の第1の実施形態に係るファイアウォール装置のディレクトリ管理機能部に設定されるサービス詳細公開ポリシーの一例を示す図である。

【図11】本発明の第1の実施形態に係るファイアウォール装置の内部ネットワークから外部ネットワークへの通信を許可するためのIPフィルタ機能部に設定されるパケットフィルタの情報を示す図である。

【図12】本発明の第1の実施形態に係るファイアウォール装置のFTPサービスの通信シーケンスと、ディレクトリ管理機能部33によってアドレス変換機能部25に設定されるアドレス変換テーブルと、IPフィルタ機能部23に設定されるパケットフィルタとを示す図である。

【図13】本発明の第1の実施形態に係るファイアウォール装置で行われる通信路設定処理の動作の一部を示すフローチャートである。

【図14】本発明の第1の実施形態に係るファイアウォール装置で行われる通信路設定処理の動作の一部を示すフローチャートである。

【図15】本発明の第1の実施形態に係るファイアウォール装置のディレクトリ管理機能部に格納されているサービス情報の一例を示す図である。

【図16】本発明の第1の実施形態に係るファイアウォール装置のディレクトリ管理機能部に設定されるサービス詳細公開ポリシーの一例を示す図である。

【図17】本発明の第2の実施形態に係る通信装置100およびそれに接続されるネットワークおよび機器の構成を示す図である。

【図18】通信装置100のネットワーク情報格納部123に格納される情報の一例を示す図である。

【図19】IEEE1394バス170に新たに被制御端末151が接続されたときの通信装置100の動作を示すシーケンス図である。

【図20】制御端末141において通信装置100から取得した制御メニューの表示の一例を示す図である。

【図21】通信装置100の個別制限項目格納部133に格納される個別制限項目の一例を示す図である。

【図22】通信装置100の個別制限項目格納部133に格納される個別制限項目の他の一例を示す図である。

【図23】制御端末141から制御メニューの要求を受けたときの通信装置100の動作を示すシーケンス図である。

【図24】通信装置100の初期制限項目格納部132に格納される初期制限項目の一例を示す図である。

【図25】通信装置100の制限項目作成部131の動作を示すフローチャートである。

【図26】制御端末141において通信装置100から

取得した制御メニューの表示の一例を示す図である。

【図 27】本発明の第 3 の実施形態に係る通信装置 1000 およびそれに接続されるネットワークおよび機器の構成を示す図である。

【図 28】IEEE1394バス 170 に新たに被制御端末 151 が接続されたときの通信装置 1000 の動作を示すシーケンス図である。

【図 29】通信装置 1000 のネットワーク情報格納部 123 に格納される情報の一例を示す図である。

【図 30】制御端末 141 から制御メニューの要求を受けたときの通信装置 1000 の動作を示すシーケンス図である。

【図 31】通信装置 1000 の個別制限項目格納部 133 に格納される個別制限項目の一例を示す図である。

【図 32】通信装置 1000 の制限項目作成部 131 の動作を示すフローチャートである。

【図 33】制御端末 141 において通信装置 1000 から取得した制御メニューの表示の一例を示す図である。

【図 34】制御端末 141 において通信装置 1000 から取得した制御メニューの表示の一例を示す図である。

【図 35】本発明の第 4 の実施形態に係る通信装置 1800 およびそれに接続されるネットワークおよび機器の構成を示す図である。

【図 36】IEEE1394バス 170 に新たに被制御端末 151 が接続されたときの通信装置 1800 の動作を示すシーケンス図である。

【図 37】通信装置 1800 のネットワーク情報格納部 123 に格納される情報の一例を示す図である。

【図 38】制御端末 141 から制御メニューの要求を受けたときの、特に、条件に合致する制限項目の数が 3 未満である場合の通信装置 1800 の動作を示すシーケンス図である。

【図 39】通信装置 1800 の個別制限項目格納部 133 に格納される個別制限項目の一例を示す図である。

【図 40】通信装置 1800 の初期制限項目格納部 132 に格納される初期制限項目の一例を示す図である。

【図 41】制御端末 141 から制御メニューの要求を受けたときの、特に、条件に合致する制限項目の数が 3 以上である場合の通信装置 1800 の動作を示すシーケンス図である。

【図 42】通信装置 1800 の制限項目作成部 1831 の動作を示すフローチャートである。

【図 43】制御端末 141 において通信装置 1800 から取得した制御メニューの表示の一例を示す図である。

【図 44】本発明の第 5 の実施形態に係る通信装置 2700 およびそれに接続されるネットワークおよび機器の構成を示す図である。

【図 45】サービス情報を取得するときの通信装置 2700 の動作を示すシーケンス図である。

【図 46】通信装置 2700 のネットワーク情報格納部

123 に格納される情報の一例を示す図である。

【図 47】制御端末 141 から制御メニューの要求を受けたときの通信装置 2700 の動作を示すシーケンス図である。

【図 48】通信装置 2700 の個別制限項目格納部 133 に格納される個別制限項目の一例を示す図である。

【図 49】通信装置 2700 の初期制限項目格納部 132 に格納される初期制限項目の一例を示す図である。

【図 50】通信装置 2700 の制限項目作成部 131 の動作を示すフローチャートである。

【図 51】従来のネットワークサービス管理方式におけるネットワークの全体構成を示す図である。

【図 52】従来のネットワークサービス管理方式においてネットワーク管理者に提供されるネットワーク情報を示す図である。

【図 53】従来のネットワークサービス管理方式においてサービス管理者に提供されるネットワーク情報を示す図である。

【図 54】従来のネットワークサービス管理方式においてユーザ端末を使用するユーザに提供されるネットワーク情報を示す図である。

#### 【符号の説明】

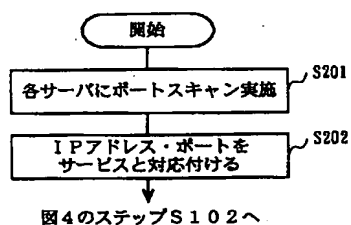
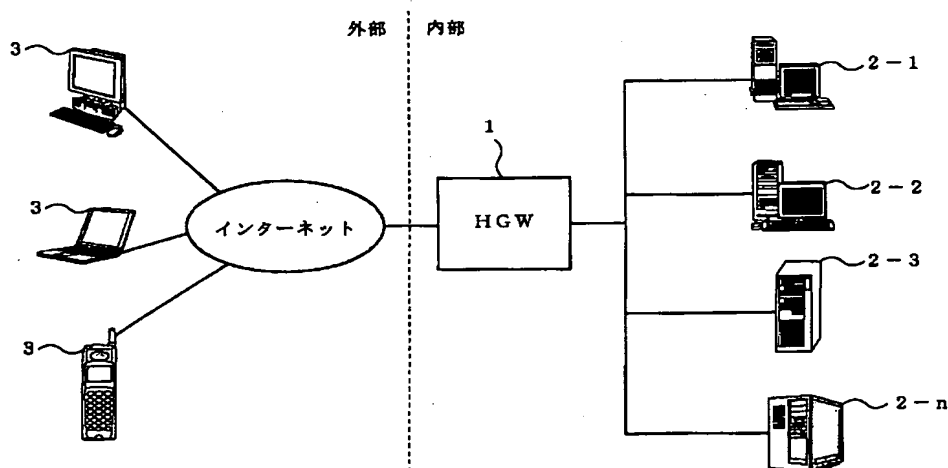
1…HGW  
2…サーバ  
3…外部端末  
10…CPU  
11、22…メモリ  
20…スイッチ部  
21…コントローラ  
23…IPフィルタ機能部  
24…フォワーディング機能部  
25…アドレス変換部  
26…PHY・MAC機能部  
31…通信部  
32…認証機能部  
33…ディレクトリ管理機能部  
34…通信路設定機能部  
100…通信装置  
110…制御メニュー構成部  
111…制御メニュー作成要求受信部  
112…制御メニュー作成部  
113…制御メニュー送信部  
120…ディレクトリ管理機能部  
121…ネットワーク構成要素検出部  
122…ネットワーク情報取得部  
123…ネットワーク情報格納部  
130…制限項目管理部  
131…制限項目作成部  
132…初期制限項目格納部  
133…個別制限項目格納部

134…入力部  
 141…制御端末  
 151、152、153…被制御端末  
 160…インターネット  
 170…IEEE1394バス  
 1000…通信装置  
 1030…制限項目管理部  
 1031…制限項目作成部  
 1054…被制御端末  
 1800…通信装置  
 1830…制限項目管理部

1831…制限項目作成部  
 2700…通信装置  
 2710…制御コマンド中継部  
 2712…制御コマンド判定部  
 2713…制御コマンド送受信部  
 2720…ディレクトリ管理機能部  
 2724…IEEE1394プロトコル変換部  
 2725…ECHONETプロトコル変換部  
 2780…インターネット  
 10 2790…ECHONET  
 2755、2756、2757…被制御端末

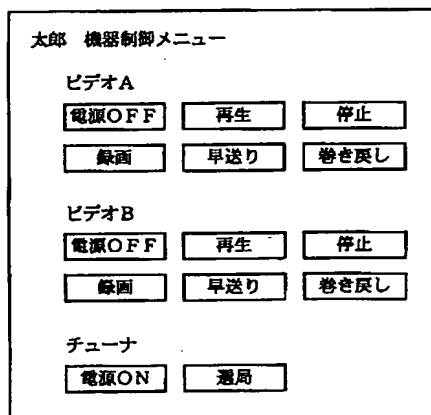
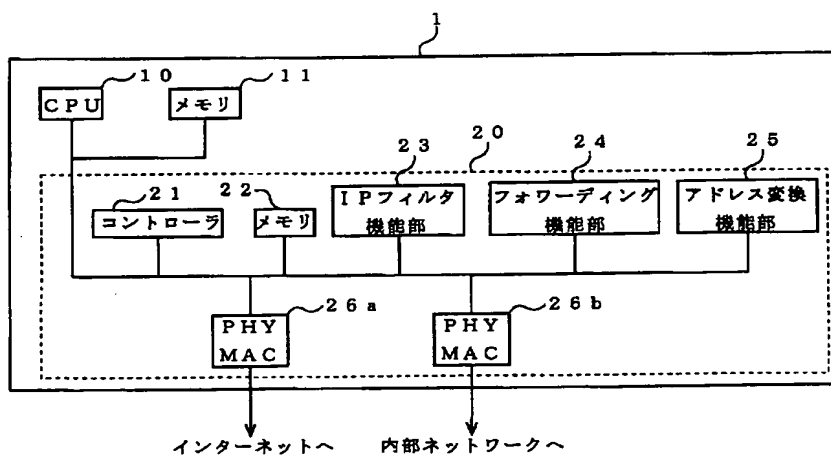
【図1】

【図13】



【図2】

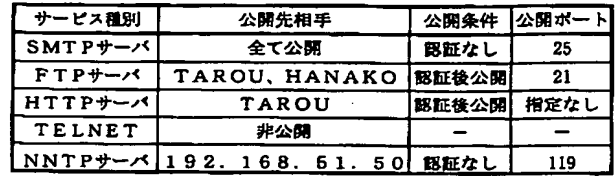
【図20】



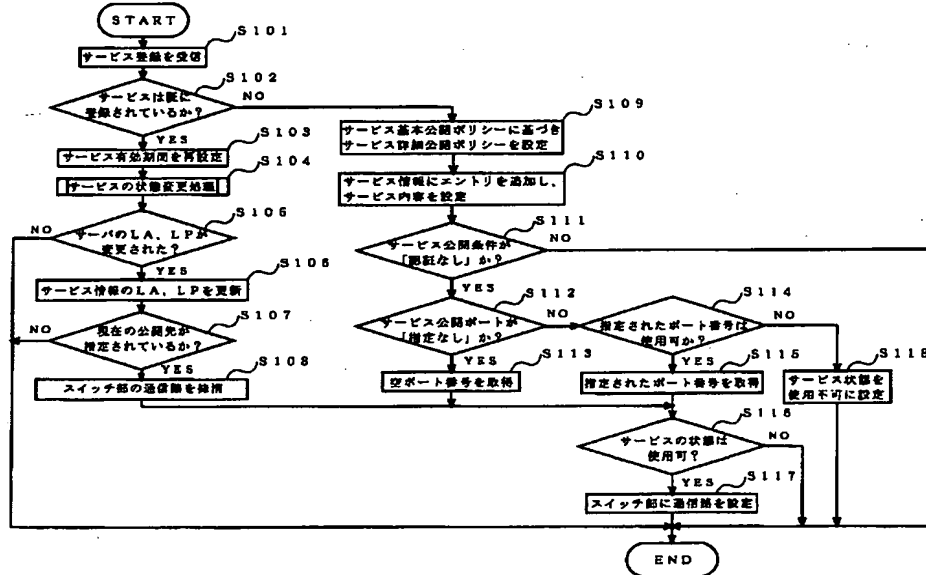
【図11】

方向	SA	DA	プロトコル	SP	DP	ACK	
外	LA	IA	TCP	LP	IP	—	デフォルト設定A
内	IA	LA	TCP	IP	LP	YES	デフォルト設定B

【图9】



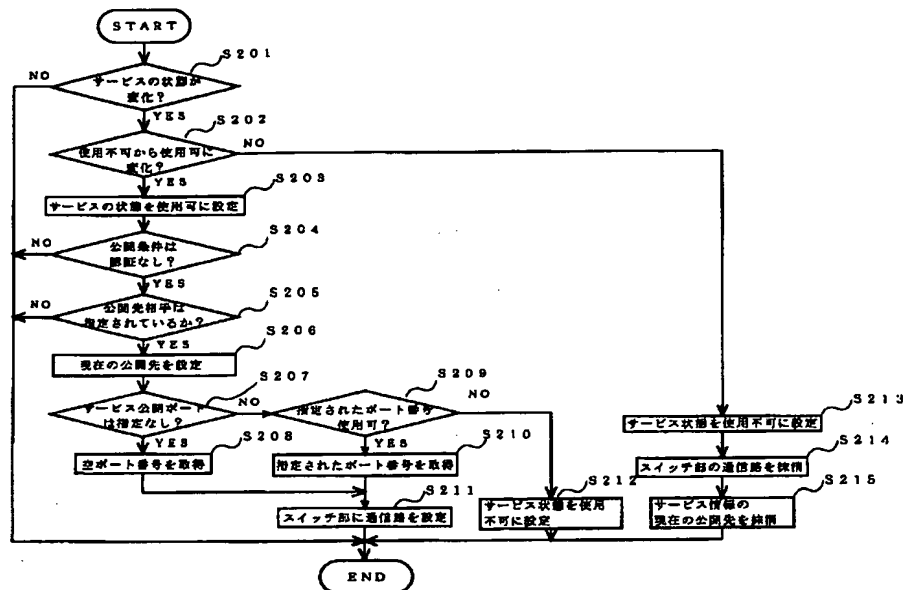
【図 4】



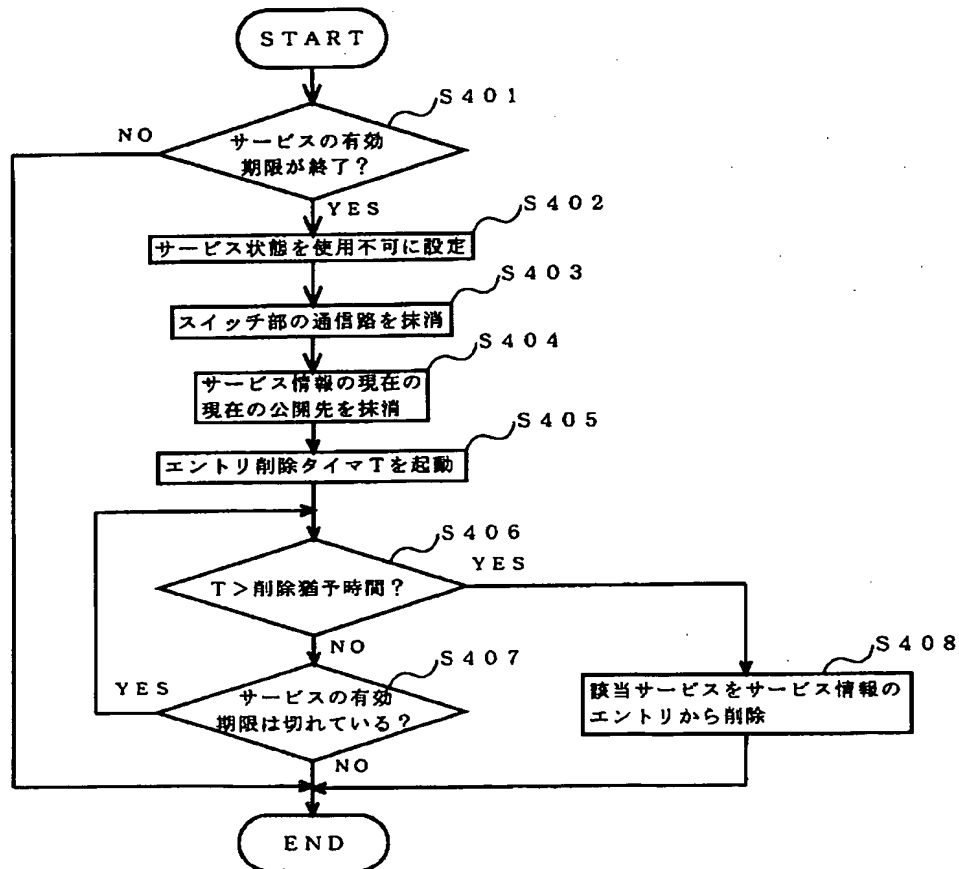
【図 8】

サービス名	サービス アドレス	プロトコル	外部公開 ポート番号	現在の公開先	サービス 有効期間	状態
SMTP	PC001 IP: LA2 PORT: 25	TCP/IP	25	全て	0:31:21	使用可
FTP	PC001 IP: LA2 PORT: 21	TCP/IP	-	-	0:31:21	使用可
HTTP	PC001 IP: LA2 PORT: 8080	TCP/IP	2048	TAROU IP: 1A1 PORT: 1025	0:31:21	使用可
FTP	PC002 IP: LA3 PORT: 21	TCP/IP	21	HANAKO IP: 1A3 PORT: 1024	0:55:35	使用可

【図5】

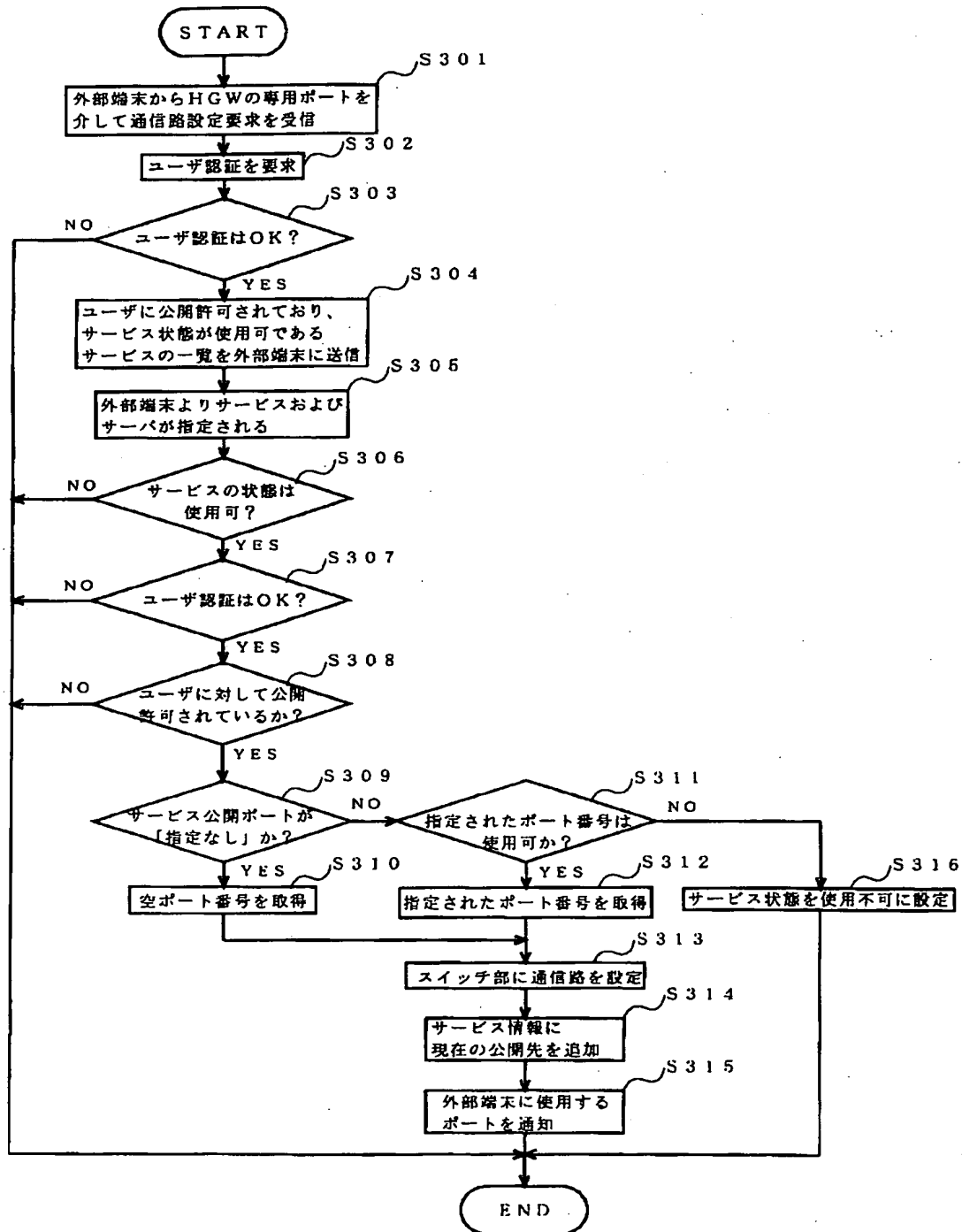


【図7】





【図6】



【図18】

GUID	機器カテゴリー	サービス情報	所属ネットワーク
0x0123456789012345	ビデオ	電源、録画、再生、早送り、巻き戻し、停止	IEEE1394
0x0123456789023456	ビデオ	電源、録画、再生、早送り、巻き戻し、停止	IEEE1394
0x0123456789034567	チューナ	電源、選局	IEEE1394

【図 10】

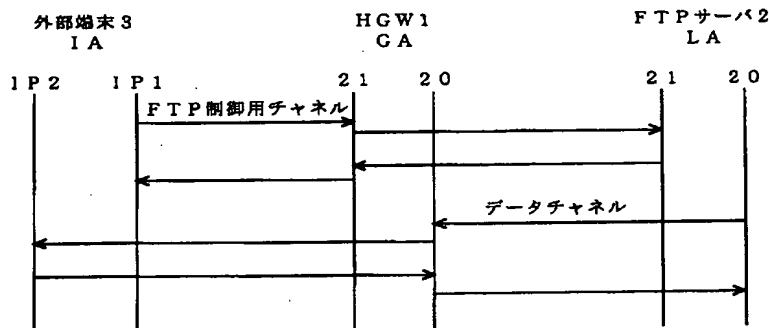
サーバ名	サービス種別	公開先相手	公開条件	公開ポート
サーバ2-1	SMTTPサーバ	全て公開	認証なし	25
	FTPサーバ	TAROU, HANAKO	認証後公開	21
	HTTPサーバ	TAROU	認証後公開	指定なし
	TELNET	非公開	-	-
サーバ2-2	FTPサーバ	HANAKO	認証後公開	21
	HTTPサーバ	HANAKO	認証後公開	指定なし
	TELNET	HANAKO	認証後公開	指定なし

【図 26】

花子 機器制御メニュー

提供可能なサービスはありません

【図 12】



(a)

(IA, IP1, GA, 21) → (IA, IP1, LA, 21) 条件C  
 (GA, 21, IA, IP1) ← (LA, 21, IA, IP1) 条件D

(b)

方向	SA	DA	プロトコル	SP	DP	ACK
内	IA	LA	TCP	IP1	21	-

条件E

(c)

【図 14】

図4のステップS102より (NOを選択)

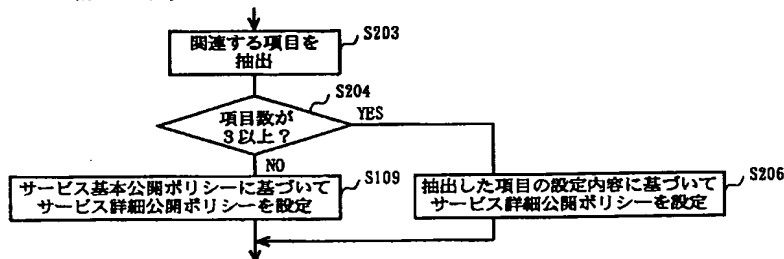
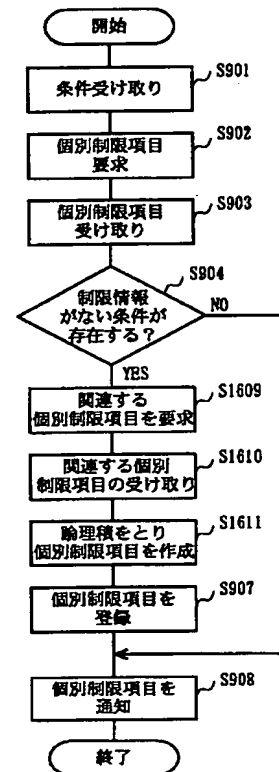


図4のステップS110へ

【図 29】

GUID	機器カテゴリー	サービス情報
0x0123456789012345	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789023456	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789034567	ビデオ	電源、録画、再生、早送り、巻き戻し、停止

【図 32】



【図 15】

サービス名	サービス アドレス	プロトコル	外部公開 ポート番号	現在の公開先	サービス 有効期間	状態
SMTP	PC001 IP:LA2 PORT:25	TCP/IP			0:31:21	使用可
FTP	PC001 IP:LA2 PORT:21	TCP/IP			0:31:21	使用可
HTTP	PC001 IP:LA2 PORT:8080	TCP/IP			0:31:21	使用可
FTP	PC002 IP:LA3 PORT:21	TCP/IP			0:56:35	使用可
FTP	PC003 IP:LA4 PORT:21	TCP/IP			0:59:55	使用可
HTTP	PC004 IP:LA5 PORT:8080	TCP/IP			0:59:55	使用可
FTP	PC004 IP:LA6 PORT:21	TCP/IP			0:59:55	使用可

新たに追加される  
サービス情報

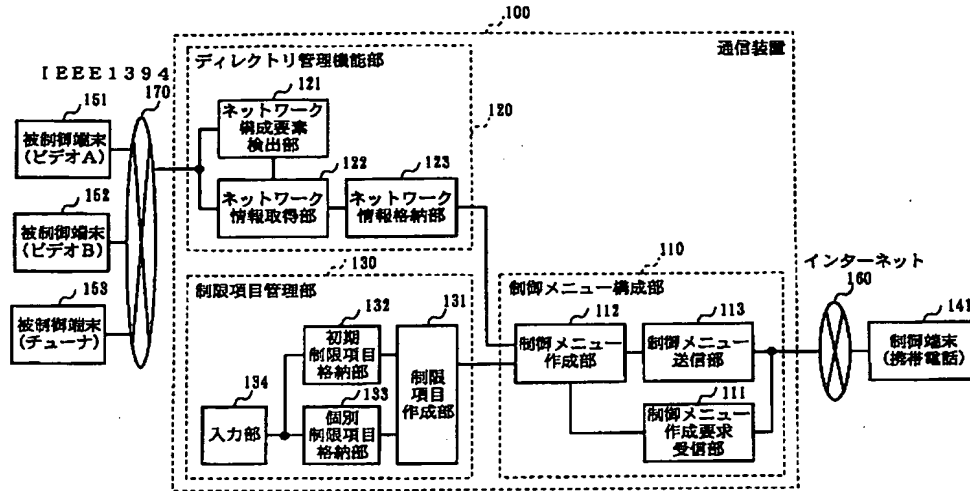
【図 16】

サーバ名	サービス種別	公開先相手	公開条件	公開ポート
サーバ2-1 項目C → 項目A →	SMTPサーバ	全て公開	認証なし	25
	FTPサーバ	TAROU, HANAKO	認証後公開	21
	HTTPサーバ	TAROU	認証後公開	指定なし
	TELNET	非公開	-	-
サーバ2-2 項目D → 項目B →	FTPサーバ	TAROU, HANAKO	認証後公開	21
	HTTPサーバ	HANAKO	認証後公開	指定なし
	TELNET	HANAKO	認証後公開	指定なし
サーバ2-3 項目E →	FTPサーバ	TAROU, HANAKO	認証後公開	21
サーバ2-4 新たに追加される 項目	HTTPサーバ	TAROU	認証後公開	指定なし
	FTPサーバ	TAROU, HANAKO	認証後公開	21

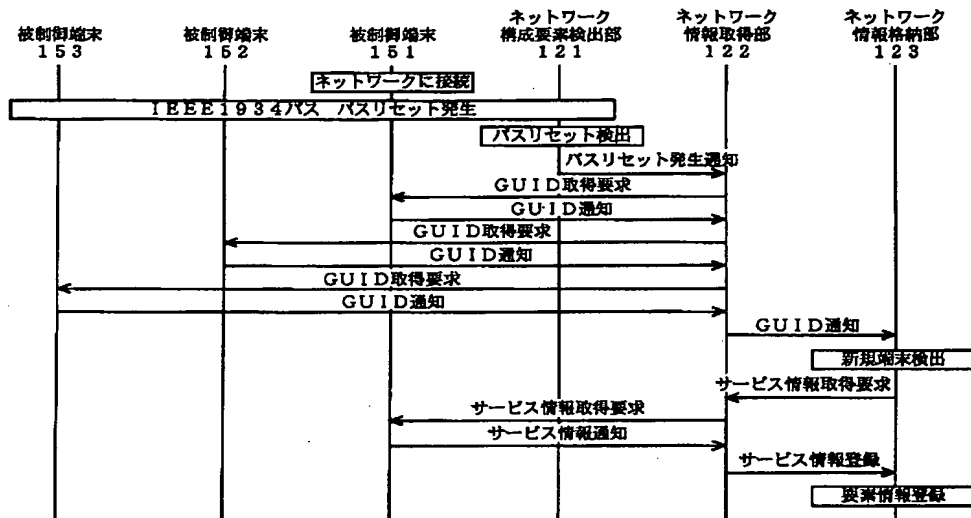
【図 21】

	GUID	ユーザID	制御端末のネットワーク	被制御端末のネットワーク	制限情報
新項目A →	0x0123456789012345	太郎	インターネット	IEEE1394	アクセス許可(1)
新項目B →	0x0123456789012345	花子	インターネット	IEEE1394	アクセス不可(0)
	0x0123456789023456	太郎	インターネット	IEEE1394	アクセス許可(1)
	0x0123456789023456	太郎	IEEE1394	IEEE1394	アクセス許可(1)
	0x0123456789023456	花子	インターネット	IEEE1394	アクセス不可(0)
	0x0123456789023456	花子	IEEE1394	IEEE1394	アクセス許可(1)
	0x0123456789034567	太郎	インターネット	IEEE1394	アクセス許可(1)
	0x0123456789034567	太郎	IEEE1394	IEEE1394	アクセス許可(1)
	0x0123456789034567	花子	インターネット	IEEE1394	アクセス不可(0)
	0x0123456789034567	花子	IEEE1394	IEEE1394	アクセス許可(1)

【図 17】



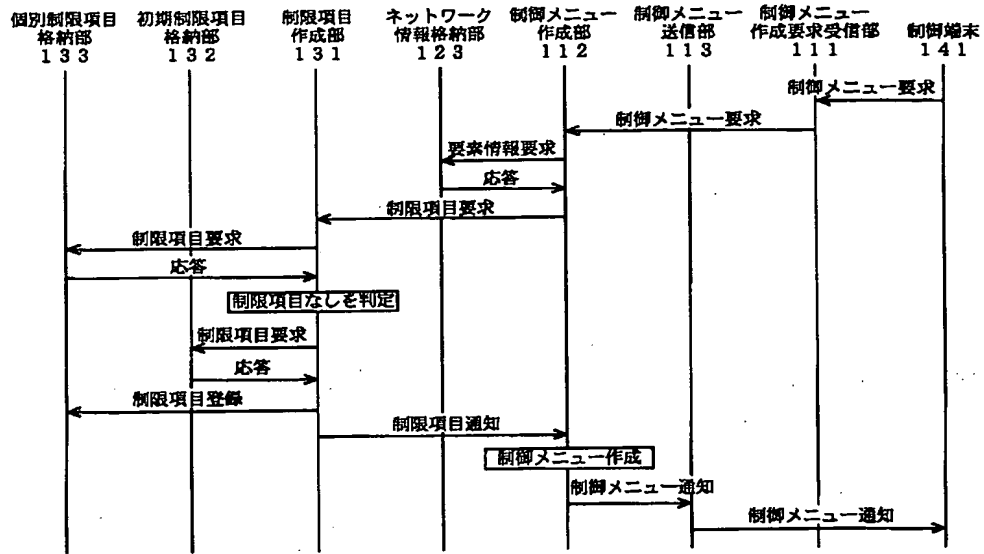
【図 19】



【図 22】

GUID	ユーザID	制御端末のネットワーク	被制御端末のネットワーク	制限情報
0x0123456789023456	太郎	インターネット	IEEE1394	アクセス許可 (1)
0x0123456789023456	太郎	IEEE1394	IEEE1394	アクセス許可 (1)
0x0123456789023456	花子	インターネット	IEEE1394	アクセス不可 (0)
0x0123456789023456	花子	IEEE1394	IEEE1394	アクセス許可 (1)
0x0123456789034567	太郎	インターネット	IEEE1394	アクセス許可 (1)
0x0123456789034567	太郎	IEEE1394	IEEE1394	アクセス許可 (1)
0x0123456789034567	花子	インターネット	IEEE1394	アクセス不可 (0)
0x0123456789034567	花子	IEEE1394	IEEE1394	アクセス許可 (1)

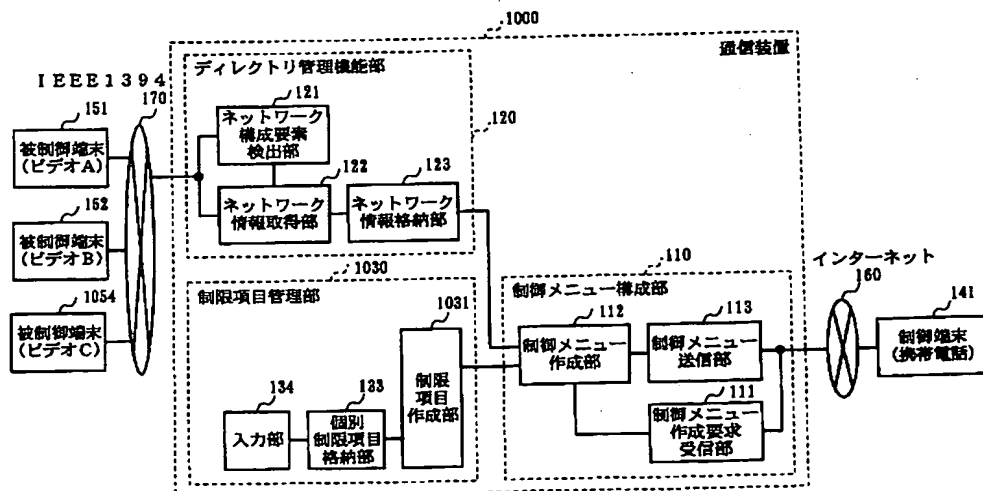
【図 23】



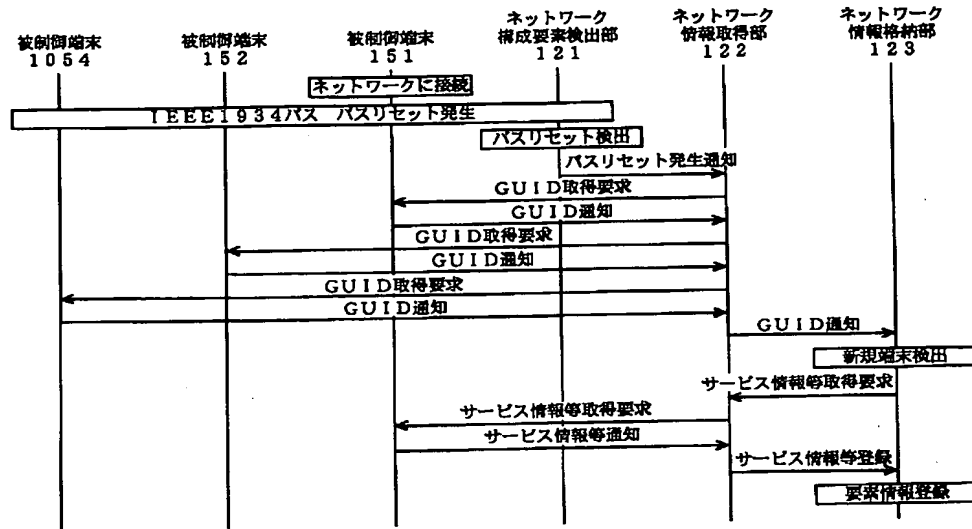
【図 24】

ユーザID	制御端末のネットワーク	被制御端末のネットワーク	制限情報
太郎	インターネット	IEEE1394	アクセス許可 (1)
太郎	インターネット	OTHER	アクセス不可 (0)
太郎	IEEE1394	IEEE1394	アクセス許可 (1)
太郎	IEEE1394	OTHER	アクセス不可 (0)
太郎	OTHER	OTHER	アクセス不可 (0)
花子	インターネット	IEEE1394	アクセス不可 (0)
花子	インターネット	OTHER	アクセス不可 (0)
花子	IEEE1394	IEEE1394	アクセス許可 (1)
花子	IEEE1394	OTHER	アクセス不可 (0)
花子	OTHER	OTHER	アクセス不可 (0)
OTHER	OTHER	OTHER	アクセス不可 (0)

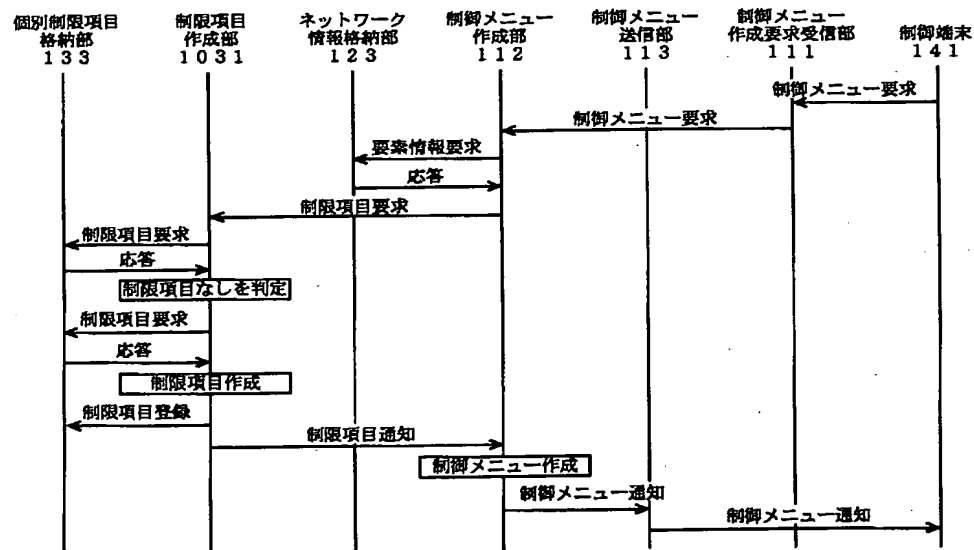
【図 27】



【図 28】



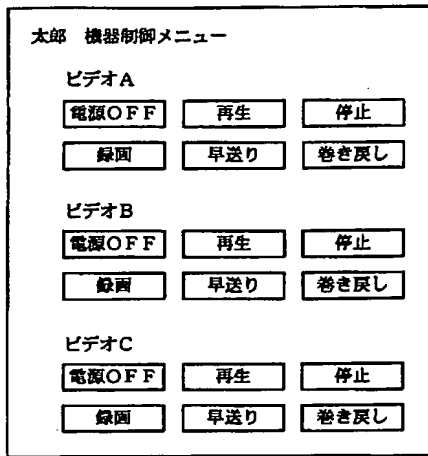
【図 30】



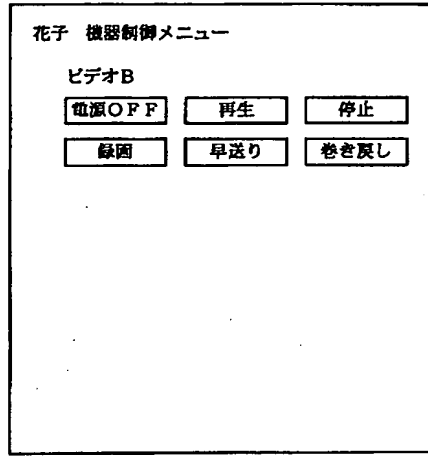
【図 31】

	GUID	ユーザID	制御端末のネットワーク	機器カテゴリー	制限情報
新項目 A →	0x0123456789012345	太郎	インターネット	ビデオ	アクセス許可 (1)
新項目 B →	0x0123456789012345	花子	インターネット	ビデオ	アクセス不可 (0)
	0x0123456789023456	太郎	インターネット	ビデオ	アクセス許可 (1)
	0x0123456789023456	太郎	IEEE1394	ビデオ	アクセス許可 (1)
	0x0123456789023456	花子	インターネット	ビデオ	アクセス不可 (0)
	0x0123456789023456	花子	IEEE1394	ビデオ	アクセス許可 (1)
	0x0123456789034567	太郎	インターネット	ビデオ	アクセス許可 (1)
	0x0123456789034567	太郎	IEEE1394	ビデオ	アクセス許可 (1)
	0x0123456789034567	花子	インターネット	ビデオ	アクセス不可 (0)
	0x0123456789034567	花子	IEEE1394	ビデオ	アクセス許可 (1)

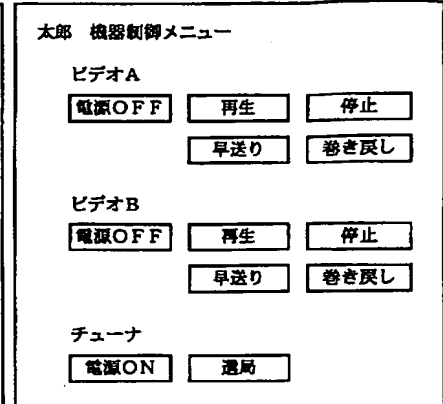
【図 3 3】



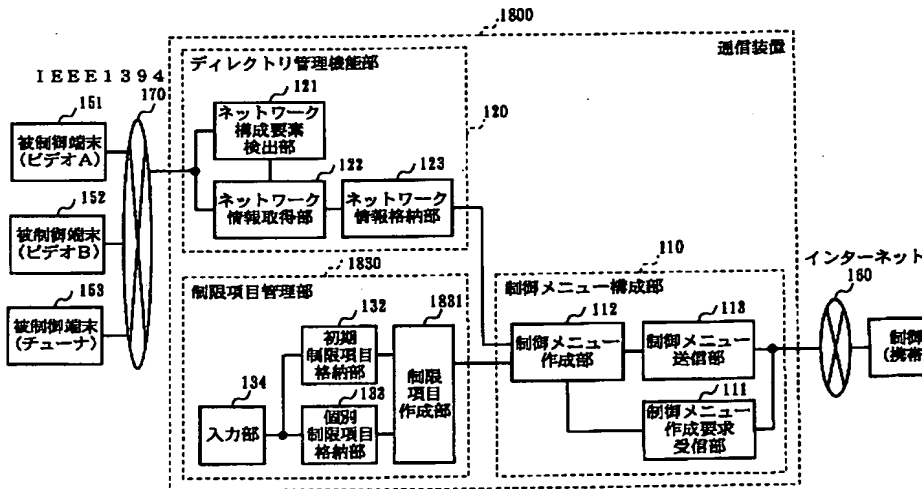
【図 3 4】



【図 4 3】



【図 3 5】



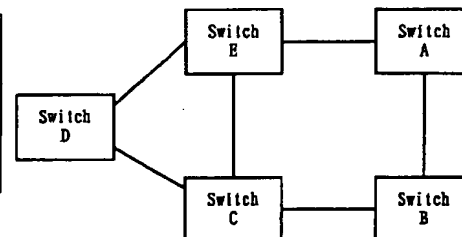
【図 3 7】

GUID	機器カテゴリー	サービス情報
0x0123456789012345	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789023456	ビデオ	電源、録画、再生、早送り、巻き戻し、停止
0x0123456789034567	チューナ	電源、選局

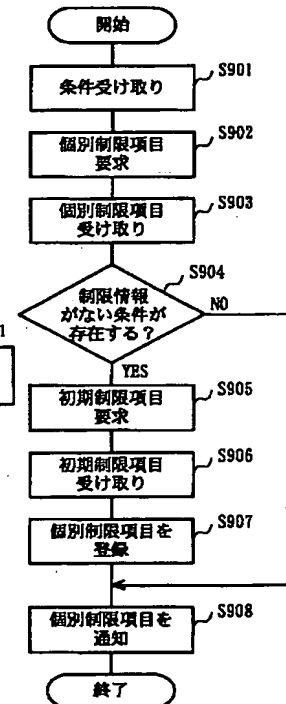
【図 4 6】

機器識別子	機器名	機器カテゴリー	サービス名	制御コマンド
0x0001	太郎のPC	PC	ファイル送信	File
0x0002	花子のチューナ	AV機器	電源	POWER
0x0002	花子のチューナ	AV機器	選局	TUNE
0x0003	1階のエアコン	空調機器	電源	POWER
0x0003	1階のエアコン	空調機器	冷房	COOL
0x0003	1階のエアコン	空調機器	暖房	HEAT

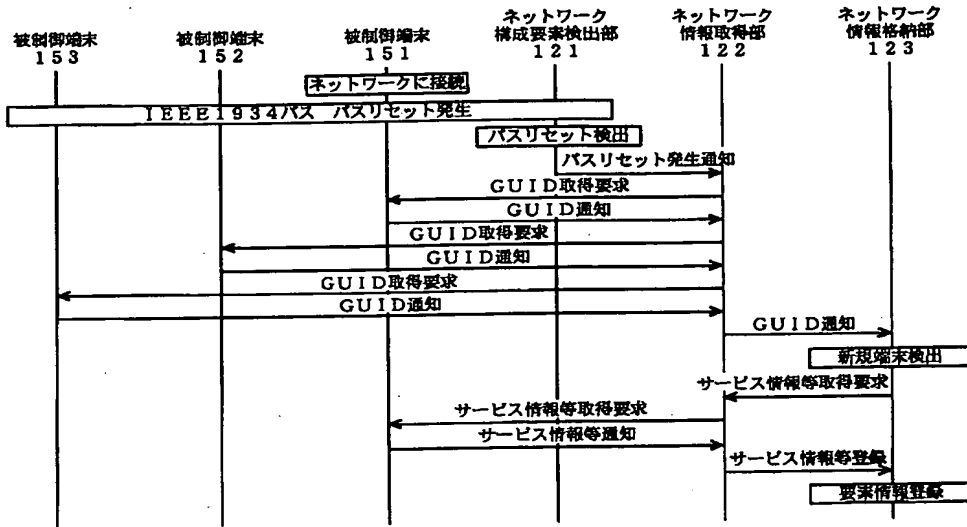
【図 5 2】



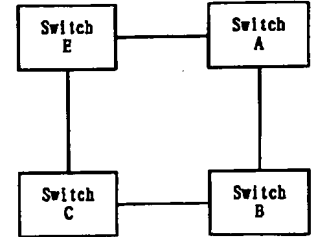
【図 5 0】



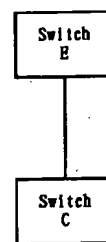
【図36】



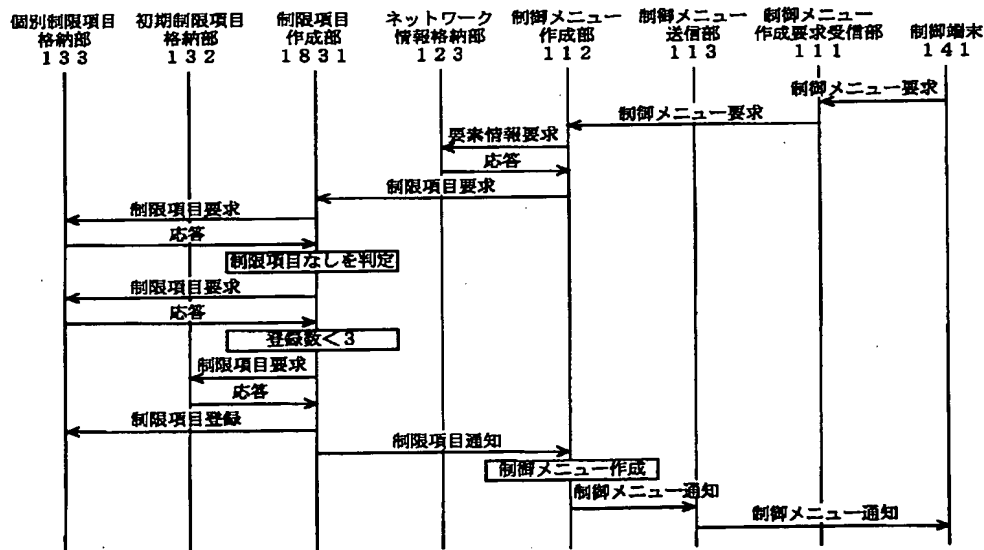
【図33】



【図34】



【図38】



【図40】

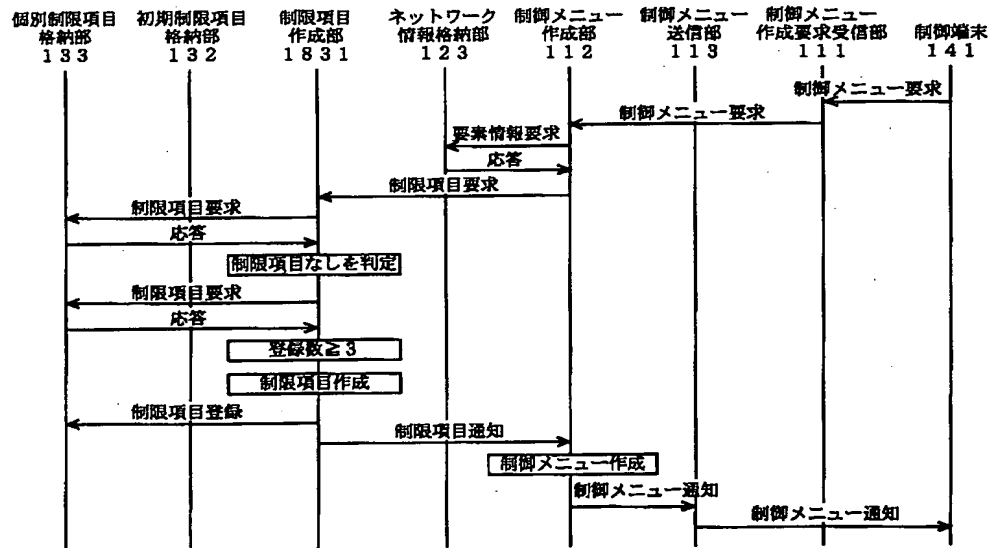
ユーザID	制御端末のネットワーク	サービス情報	制限情報
太郎	インターネット	電源	アクセス許可 (1)
太郎	インターネット	録画	アクセス不可 (0)
太郎	インターネット	再生	アクセス許可 (1)
太郎	インターネット	早送り	アクセス許可 (1)
太郎	インターネット	巻き戻し	アクセス許可 (1)
太郎	インターネット	停止	アクセス許可 (1)
太郎	インターネット	通局	アクセス許可 (1)
太郎	インターネット	OTHER	アクセス不可 (0)
太郎	IEEE1394	OTHER	アクセス許可 (1)
OTHER	OTHER	OTHER	アクセス不可 (0)



【図 39】

	GUID	ユーザID	制御端末のネットワーク	サービス情報	制限情報
新項目 A →	0x0123456789012345	太郎	インターネット	電源	アクセス許可 (1)
新項目 B →	0x0123456789012345	太郎	インターネット	録画	アクセス不可 (0)
新項目 C →	0x0123456789012345	太郎	インターネット	再生	アクセス許可 (1)
新項目 D →	0x0123456789012345	太郎	インターネット	早送り	アクセス許可 (1)
新項目 E →	0x0123456789012345	太郎	インターネット	巻き戻し	アクセス許可 (1)
新項目 F →	0x0123456789012345	太郎	インターネット	停止	アクセス許可 (1)
	0x0123456789023456	太郎	インターネット	電源	アクセス許可 (1)
	0x0123456789023456	太郎	インターネット	録画	アクセス不可 (0)
	0x0123456789023456	太郎	インターネット	再生	アクセス許可 (1)
	0x0123456789023456	太郎	インターネット	早送り	アクセス許可 (1)
	0x0123456789023456	太郎	インターネット	巻き戻し	アクセス許可 (1)
	0x0123456789023456	太郎	インターネット	停止	アクセス許可 (1)
	0x0123456789023456	太郎	IEEE1394	OTHER	アクセス許可 (1)
	0x0123456789034567	太郎	インターネット	電源	アクセス許可 (1)
	0x0123456789034567	太郎	インターネット	選局	アクセス許可 (1)
	0x0123456789034567	太郎	IEEE1394	OTHER	アクセス許可 (1)

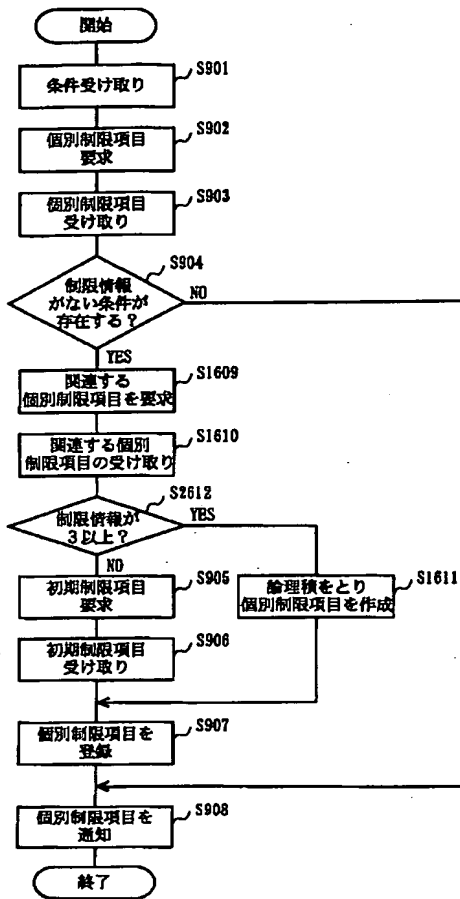
【図 41】



【図 48】

	機器識別子	制御端末のネットワーク	被制御端末のネットワーク	制限情報
	0x0001	宅外	宅内	アクセス不可 (0)
	0x0001	宅内	宅内	アクセス許可 (1)
	0x0002	宅外	宅内	アクセス許可 (1)
	0x0002	宅外	宅内	アクセス許可 (1)
新項目 A →	0x0003	宅外	宅内	アクセス許可 (1)

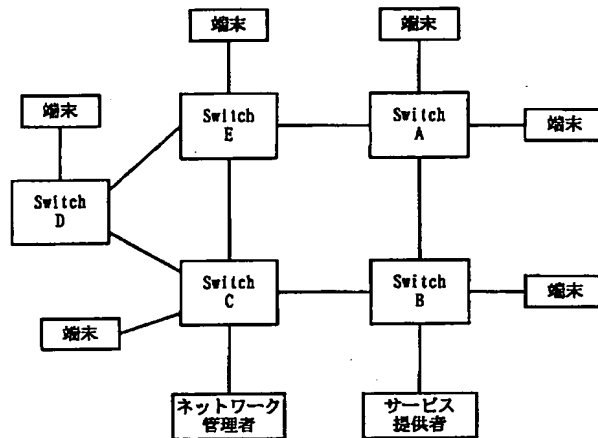
【図42】



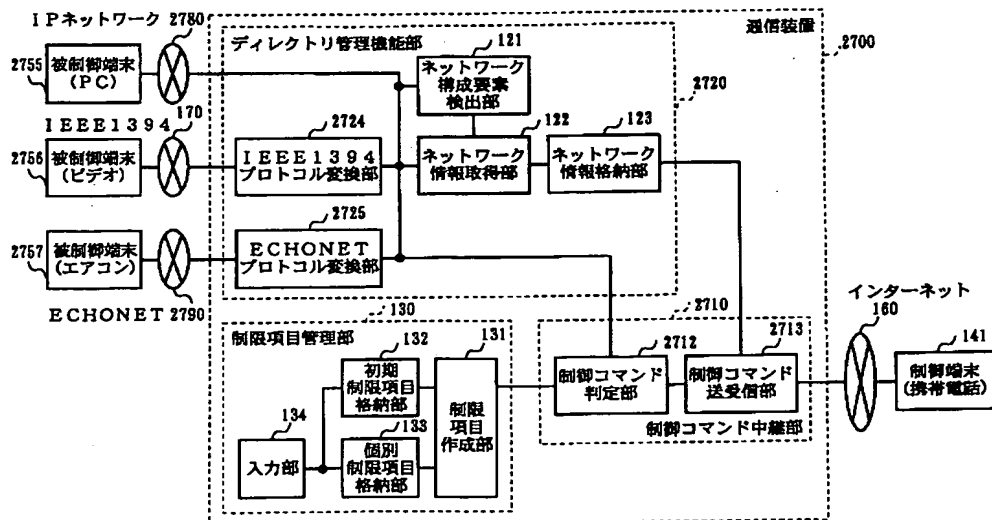
【図49】

制御端末のネットワーク	被制御端末のネットワーク	機器カテゴリー	制限情報
宅外	宅内	PC	アクセス不可 (0)
宅外	宅内	AV機器	アクセス許可 (1)
宅外	宅内	空調機器	アクセス許可 (1)
宅内	宅内	PC	アクセス許可 (1)
宅内	宅内	AV機器	アクセス許可 (1)
宅内	宅内	空調機器	アクセス許可 (1)

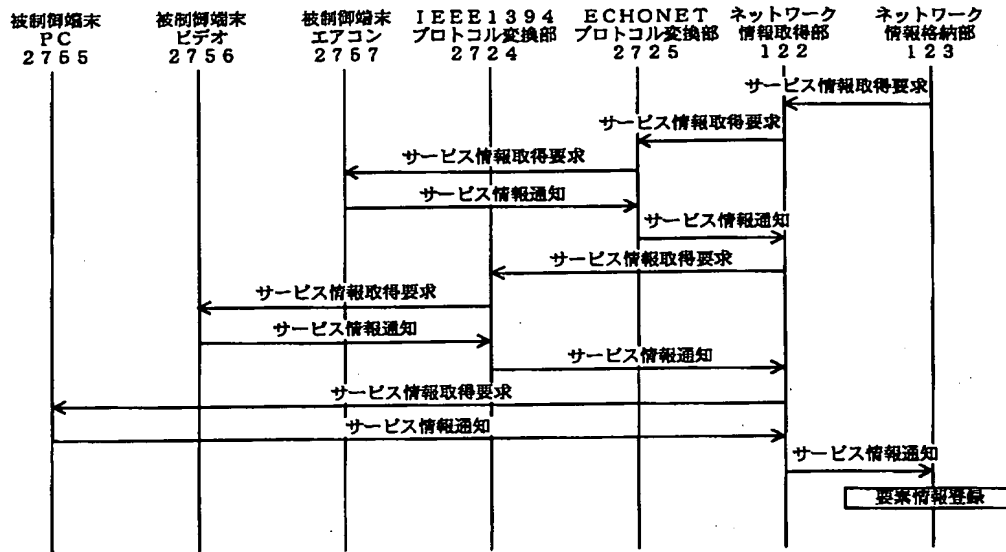
【図51】



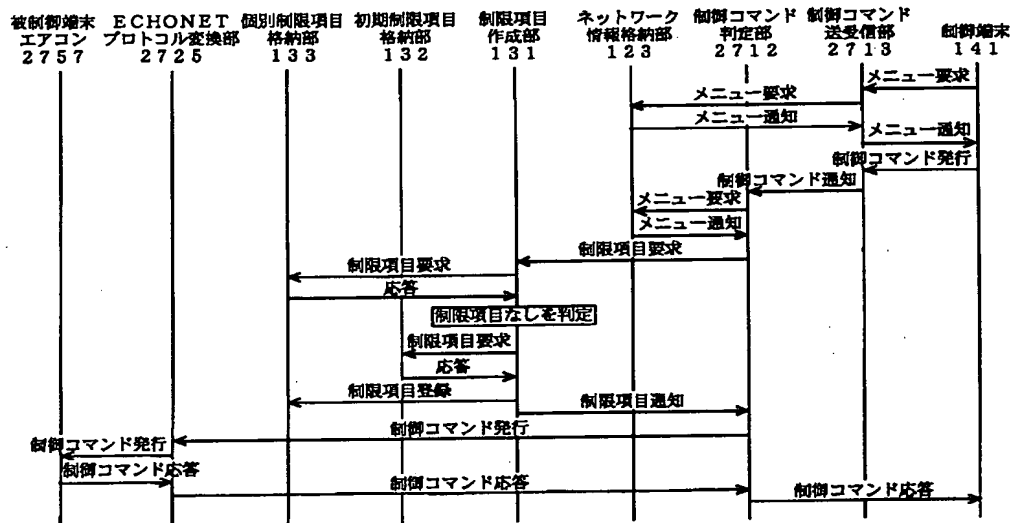
【図44】



【図 45】



【図 47】



フロントページの続き

(72) 発明者 久保田 幸司  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72) 発明者 斉藤 孝弘  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 石川 博一  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
Fターム(参考) 5B085 AE00 AE02 BC02  
5B089 KA17 KB13  
5K030 GA15 HD03 HD06 HD09 LD20  
5K033 AA08 CB09 DA06 DB18